MEMORIAS

SEGUNDO TALLER DE TEORÍA DE NÚMEROS DEL CENTRO–SURESTE

XALAPA–EQZ., VER.
Abril 2007

Facultad de Matemáticas
Universidad Veracruzana

MEMORIAS

SEGUNDO TALLER DE TEORÍA DE NÚMEROS DEL CENTRO-SURESTE

XALAPA-EQZ., VER.
Abril 2007

Facultad de Matemáticas
Universidad Veracruzana

UNIVERSIDAD AUTONOMA METROPOLITANA
Casa abierta al tiempo Azcapotzalco

Universidad Veracruzana

ISBN: 978-970-31-933-3

Sección de producción
y distribución editoriales
Tel. 5318-9222 / 9223
Fax 5318-9222

Universidad Autónoma Metropolitana
Unidad Azcapotzalco
Av. San Pablo 180
Col. Reynosa Tamaulipas
Delegación Azcapotzalco
C.P. 02200
México, D.F.

1a. edición, 2007
Impreso en México.

Comité Organizador

Dr. José Rigoberto Gabriel Argüelles	Universidad Veracruzana
Dr. Raquiel Rufino López Martínez	Universidad Veracruzana
Dr. Josue Ramírez Ortega	Universidad Veracruzana
Dr. Mario Pineda Ruelas	Universidad Autónoma Metropolitana
M. en C. Rogelio Herrera Aguirre	Universidad Autónoma Metropolitana
Dr. Arturo Cueto Hernández	Universidad Autónoma Metropolitana

Editor

Dr. Arturo Cueto Hernández

Contenido

Prólogo

Ha pasado poco más de un año de que realizamos el Primer Taller de Teoría de Números del Centro–Sureste en la Facultad de Matemáticas de la Universidad Veracruzana situada en la Atenas veracruzana, Xalapa–Eqz. Los augurios para este evento no eran prometedores; pero gracias al profesionalismo con que asumieron los expositores este evento y la respuesta que dieron para hacer posible la edición de las Memorias del mismo, permitieron tener apoyos más francos para llevar a cabo el Segundo Taller de Teoría de Números del Centro–Sureste en el mes de abril del presente año.

Recordemos que el Taller tiene por finalidad contribuir a una formación integral de los alumnos de la Licenciatura en Matemáticas de la Facultad de Matemáticas de la Universidad Veracruzana. Este año se presentó una nueva oportunidad –algunos dirían un reto–: contribuir a la formación de los alumnos de la Maestría en Matemática Educativa que imparte la Facultad de Matemáticas, presentando temas de interés para personas que no son matemáticos, pero que por su actividad profesional tratan con un aspecto importante de la matemática, su enseñanza.

Dados los requerimientos del Taller, conferencias para los alumnos de la licenciatura y maestría, estos propiciaron el crecimiento en el número de conferencias; pero lo más importante, contar con la participación de colegas de otras instituciones, como el CINVESTAV del I.P.N. y la Universidad Autónoma del Estado de Hidalgo. Así, en el mes de abril en la ciudad de Xalapa tuvimos tres días de actividad académica con una participación entusiasta por parte de los alumnos y los conferencistas –fuego amigo, pero divertido– en un ambiente sumamente agradable. No todas las conferencias fueron propiamente de Teoría de Números, pero sin duda enriquecieron el evento. Creemos que la realización del Taller realmente cumple con su finalidad, y esto lo justifica.

Debemos reconocer y agradecer a todos aquellos que contribuyeron a la realización de este Segundo Taller de Teoría de Números del Centro–Sureste: primero a los alumnos por su entusiasta participación ya que ellos han sido la razón para llevarlo a cabo; sin su compromiso, no habría tenido sentido (esperamos no haberlos defraudado). A nuestros colegas conferencistas, ¡gracias por la calidad de sus presentaciones! Al personal docente y administrativo de la Facultad de Matemáticas de la Universidad Veracruzana, por su apoyo logístico y buena disposición, y por último y no menos importante, queremos agradecer a las autoridades tanto de la Universidad Veracruzana como de la Universidad Autónoma Metropolitana–Azcapotzalco

por el apoyo económico y las facilidades para la realización del Taller; en particular, al M. en C. José Ángel Rocha Martínez, Director de la División de Ciencias Básicas e Ingeniería de la Universidad Autónoma Metropolitana–Azcapotzalco, por el apoyo brindado a estos eventos durante su gestión. ¡En hora buena José Ángel, y éxito en lo que emprendas!

Esperamos que estas Memorias den constancia de que nuestras instituciones cumplen cabalmente con dos de sus funciones, la preservación y la difusión de la cultura; en este caso, de la matemática. Reitero, muchas gracias a todos los que hicieron posible el Taller. Cualquier omisión o error es responsabilidad del que escribe estas líneas.

Arturo Cueto Hernández

México D.F., septiembre 2007

PRIMERA PARTE

SECCIÓN

LICENCIATURA

Fracciones Continuas

Raúl Amezcua Gómez
Universidad Autónoma Metropolitana–Azcapotzalco
Departamento de Ciencias Básicas
Av. San Pablo No. 180,
Col. Reynosa Tamaulipas
Azcapotzalco
02200 México, D.F.
rag@correo.azc.uam.mx

La teoría de fracciones continuas trata con un algoritmo especial que es una de las herramientas más importantes en análisis, teoría de la probabilidad y, especialmente, en la teoría de números. El propósito de la presente exposición es dar un panorama solamente con las llamadas fracciones continuas simples, esto es, aquellas con la forma

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}}$$

en donde $a_0, a_1, a_2, a_3, \ldots$ son usualmente números enteros positivos, y llamados *cocientes parciales o términos*. El número de cocientes parciales puede ser finito o infinito.

Por conveniencia escribamos la fracción continua de arriba como

$$[a_0; a_1, a_2, \ldots]$$

En caso de una fracción continua finita

$$[a_0; a_1, a_2, \ldots, a_n]$$

diremos que su orden es igual a n.

Llamaremos a la fracción continua

$$[a_0; a_1, a_2, \ldots, a_k]$$

donde $0 \leq k \leq n$, un *segmento* de la fracción continua finita de arriba. También llamemos a

$$[a_k; a_{k+1}, \ldots, a_n]$$

un *residuo* de la misma fracción continua finita de orden n.

Denotaremos por p_k/q_k la representación del segmento

$$[a_0; a_1, a_2, \ldots, a_k]$$

de la fracción continua, y lo llamaremos el *k–ésimo convergente* de la fracción continua. Para una fracción continua α de orden n, se tiene

$$\frac{p_n}{q_n} = \alpha$$

Teorema 1. *(Regla para formar convergentes). Para cualquier $k > 2$,*

$$p_k = a_k p_{k-1} + p_{k-2}$$

$$q_k = a_k q_{k-1} + q_{k-2}$$

Teorema 2. *Para toda $k \geq 0$,*

$$q_k p_{k-1} - p_k q_{k-1} = (-1)^k$$

Corolario 1. *Para toda $k \geq 1$,*

$$\frac{p_{k-1}}{q_{k-1}} - \frac{p_k}{q_k} = \frac{(-1)^k}{q_k q_{k-1}}$$

Teorema 3. *Para toda $k \geq 1$,*

$$q_k p_{k-2} - p_k q_{k-2} = (-1)^{k-1} a_k$$

Corolario 2. *Para toda $k \geq 1$,*

$$\frac{p_{k-2}}{q_{k-2}} - \frac{p_k}{q_k} = \frac{(-1)^{k-1} a_k}{q_k q_{k-2}}$$

Esto muestra que los convergentes de orden par forma una sucesión creciente y los de orden impar decreciente.

Teorema 4. *Convergentes de orden par forman una secuencia creciente y convergentes de orden impar una secuencia decreciente. También, cada convergente de orden impar es mayor que cualquier convergente de orden par.*

Teorema 5. *El valor de α de la fracción continua infinita $[a_0; a_1, a_2, \ldots]$ para cualquier $k \geq 0$ satisface*

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{q_k q_{k+1}}$$

Teorema 6. *Para toda $k \geq 0$*

$$\left|\alpha - \frac{p_k}{q_k}\right| > \frac{1}{q_k(q_{k+1} + q_k)}$$

Teorema 7. *Para todo número real corresponde una única fracción continua con valor igual a α. Esta fracción es finita si α es racional e infinita si α es irracional.*

Teorema 8. *La desigualdad*

$$\left|\alpha - \frac{p}{q}\right| < \frac{c}{q^2}$$

tiene un conjunto infinito de soluciones en los enteros p y q, $q > 0$, dado cualquier α si $c > 1/\sqrt{5}$. Sin embargo, si c es menor habrá un número finito de soluciones.

Teorema 9. *Para cualquier función positiva $\varphi(q)$ con argumento entero q, existe un irracional α tal que la desigualdad*

$$\left|\alpha / \frac{p}{q}\right| < \varphi(q)$$

tiene un conjunto infinito de soluciones en los enteros p y q, $q > 0$.

Teorema 10. *Para todo número irracional con términos acotados, y para una c suficientemente pequeña la desigualdad*

$$\left|\alpha - \frac{p}{q}\right| < \frac{c}{q^2}$$

no tiene soluciones en los enteros p y q, $q > 0$. Por otro lado, dado cualquier α con una sucesión no acotada de términos y una arbitraria $c > 0$, la desigualdad tiene un conjunto infinito de tales soluciones.

Suponga que

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

es un polinomio de grado n con coeficientes enteros $a_0, a_1, \ldots, a_n$. Entonces, una raíz, α, de este polinomio se dice algebraica, y si no satisface ser raíz de otro polinomio de grado menor se dice de grado n. En particular, los racionales son números algebraicos de grado 1. $\sqrt{2}$ es de grado 2, o irracional cuadrático. Todo número no algebraico se dice trascendente, por ejemplo, e y π.

Teorema 11. *(Liouville) Para cualquier número algebraico irracional α de grado n, existe un número positivo C tal que para cualesquiera p y q $(q > 0)$,*

$$\left|\alpha - \frac{p}{q}\right| > \frac{C}{q^n}$$

Este teorema muestra que los números algebraicos no admiten aproximaciones fraccionales racionales mayores a cierto orden de precisión (dependiendo básicamente del grado del número algebraico en cuestión). La principal importancia histórica de este teorema consistió en el hecho de hacer posible la prueba de la existencia de números trascendentes, y permitió dar ejemplos específicos de tales números. Para esto, es suficiente exhibir un irracional para el cual hay una fracción racional extremadamente cercana, y el teorema 9 muestra que las posibilidades son ilimitadas.

Específicamente, el último teorema muestra que si para cualquier $C > 0$ y un natural n arbitrario existen enteros p y q $(q > 0)$, tal que

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{C}{q^n}$$

entonces el número α es trascendente. Usando el aparato de fracciones continuas, es posible exhibir tantos de estos números como se desee. Todo lo que se requiere es elegir términos $a_0, a_1, a_2, \ldots, a_k$ para formar convergentes p_k/q_k, y tomar

$$a_{k+1} > q_k^{k-1}$$

ya que

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q_k q_{k+1}} < \frac{1}{q_k^2 a_{k+1}} < \frac{1}{q_k^{k+1}}$$

Resultado de lo anterior, es que la desigualdad

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{C}{q^n}$$

es obviamente satisfecha para valores k suficientemente grandes, sin importar que $C > 0$ y natural n sean.

El **Teorema de Liouville** muestra que, para un número α irracional cuadrático, existe un entero positivo C, que depende de α, tal que la desigualdad

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{C}{q^2}$$

no tiene solución en enteros p y q ($q > 0$). De esto y del Teorema 10, se sigue que los elementos de un número irracional cuadrático están acotados. Sin embargo, Lagrange descubrió antes la más significativa propiedad de estos irracionales cuadráticos: la sucesión de sus elementos es periódica, y viceversa, toda fracción continua periódica representa algún número irracional cuadrático.

Referencias

[1] H. Davenport, *The Higher Arithmetic*, London, Hutchinson's University Library, 1952.

[2] G. Hardy y E. Wright, *An Introduction to de Theory of Numbers*, Oxford, Clarendon Press, 1960.

[3] A. Khinchin, *Continued Fractions*, N. Y., Dover, 1997.

[4] L. Lorentzen y H. Waadeland, *Continued Fractions with Applications*, Amsterdam, North-Holland, 1992.

[5] I. Niven, Numbers: *Rational and Irrational*, New Mathematical Library 1, New York, Random House Inc., 1961.

[6] I. Niven y H. Zuckerman, *Introducción a la Teoría de los Números*, D.F., Limusa-Wiley, S.A., 1969.

[7] C. Olds, *Continued Fractions, New Mathematical Library 9*, New York, 1963.

[8] I. Vinográdov *Fundamentos de la Teoría de los Números*, URSS, Mir, 1987.

Problema del Logaritmo Discreto en Campos Finitos

Ricardo López Bautista
Universidad Autónoma Metropolitana–Azcapotzalco
Departamento de Ciencias Básicas
Av. San Pablo No. 180,
Col. Reynosa Tamaulipas
Azcapotzalco
02200 México, D.F.
rlopez@correo.azc.uam.mx

1. Problema del logaritmo discreto

Definición: Sea G grupo finito. $g, \mu = g^x \in G$. El número $x = \text{Log}_g(\mu)$ se llamará Logaritmo discreto de μ en base g.

Campos finitos

Sea p un número primo, n un número natural. Por $\mathbb{F}_{p^n}$ denotaremos al campo finito de p^n elementos.

Se tiene que:

1. $\mathbb{F}_{p^n}$ es el campo de descomposición de:
$$x^{p^n} - x.$$
2. $$\mathbb{F}^*_{p^n} = < \lambda >, \quad \mathbb{F}_{p^n} = \mathbb{F}_p(\lambda).$$

El problema del logaritmo discreto en campos finitos, se plantea así:

Sea F campo finito. $F^* = < \lambda >$, $b \in F^*$.

Problema: Encuentre el mínimo natural r tal que:
$$\lambda^r = b.$$
$$r = \text{Log}_\lambda(b).$$

El problema del logaritmo discreto en campos finitos, es un problema no resuelto

Logaritmo discreto en cuales campos finitos?

1. $\text{Log}_\lambda(b)$, $\quad b \in \mathbb{F}_{p^n}$.
   Logaritmo discreto en campos finitos $\mathbb{F}_{p^n}$.

2. $\text{Log}_\lambda(b)$, $\quad b \in \mathbb{F}_p$.
   Gordon, D.M., Discrete Logaritms in $GF(p)$ using the number field sieve.

Ejemplo 1.

1. $$Log_2(8) = 3, \text{ pues } 2^3 = 8.$$

2. En $\mathbb{F}_{127}$, $3^{57} = 157004289908208161164053456 3 \equiv 77 \pmod{127}$.

$$57 = Log_3(77).$$

Ejemplo 2.

Trivialidades e ¿imposibles?

1. Trivial encontrar los números: $2239^2, 2239^3, 2239^5, 2239^{11}, 2239^{13}, 2239^{17}, 2239^{19}, 2239^{23}, 2239^{29}$.

2. Difícil el problema inverso?
   Dado

$$p = 3108193812051968080419610101196426101966141219110309197118053775 9$$

$log_{2239}\{2, 3, 5, 11, 13, 17, 19, 23, 29\} \pmod{p}$:

$$\begin{aligned}
&1294905077901917941090643111144342403004027405671868406989835\blacksquare\\
&8344220885634977691869506785685387873400846925384314417497147\blacksquare\\
&7793979290203354230008928554004085354267913160264528405127775\blacksquare\\
&3406053575619699456246678719616780841117153738097562617397853\blacksquare\\
&3015487238013169421515671698658816325798119770300617375012366\blacksquare\\
&6829508421414990997759481528214430875824129363346136248248839\blacksquare\\
&2613553427439878220576700078429636267167937064246496633630990\blacksquare\\
&1802482076078135242510845697458291541721272172020346763120224\blacksquare\\
&7942954244416950195278458550767759322991902860684033069907666\blacksquare\\
&5370719512879434329223306409668707388 07\blacksquare
\end{aligned}$$

Cribas: campos de funciones, campos numéricos

Logaritmo discreto aparece en varios esquemas criptografícos.

1. Intercambio de llave Diffie-Hellman.
2. Criptosistema ElGamal, esquema de firma digital ElGamal y Schnorr.

Se han trabajado diversos grupos:

1. En campos finitos.
2. Curvas elípticas.
3. Curvas hiperelípticas.

Para que sirve el problema del logaritmo discreto en campos finitos?

1. Ataques a criptosistemas se basan sobre el logaritmo discreto en campos finitos.
2. Problema del Logaritmo discreto (DLP) aparece en criptografía.
3. Tópico en Matemáticas.
4. Seguridad. Diffie, Hellman, ElGamal, Esquema de firma digital.

Algoritmos subexponenciales para resolver el problema del logaritmo discreto

1. $\mathbb{F}_p$: Criba en campos numéricos. (Gordon, Shirokauer).
2. $\mathbb{F}_{2^n}$: Criba en campos de funciones. (Adleman, Coppersmith)

Exitos alcanzados

1. $\mathbb{F}_{2607}$.
2. Usando criba en campos de funciones, Joux y Lercier resuelto en $\mathbb{F}_{2521}$.

Definición 1. *Sea* $\mathbb{B} \subseteq \mathbb{F}_2[x]$. $\pi \in \mathbb{F}_2[x]$ *se dice* $\mathbb{B}$*–suave si* π_i *se factoriza en* $\mathbb{B}$.

Coppersmith. Logaritmo discreto en $\mathbb{F}_{2^n}$.

[1]
$$\mathbb{F}_{2^n} \cong \frac{\mathbb{F}_2[x]}{< f(x) >}.$$

[2] $f(x) \in \mathbb{F}_2[x]$ polinomio irreducible, $\deg f(x) = n$.

[3] $f(x) = x^n + f_1(x)$ irreducible.

[4] $f_1(x)$ de grado pequeño.

[5]
$$2^r \cong n^{1/3}.$$

[6]
$$h := \left\lceil \frac{n}{2^r} \right\rceil.$$

[7] Selección de la base de factores:

$$\mathbb{B} = \{\pi_i \in \mathbb{F}_2[x] | \pi_i \text{ polinomios irreducibles, } \deg \pi_i \leq b\}.$$

[8] Seleccione $\left(\frac{2^{b+1}}{b}\right)$ relaciones entre los π_i^s.

[9] Calcule $Log(\pi_i)$ como la solución de un sistema lineal.

[10] $\mathbb{B}$ es escogido suficientemente grande tal que es fácil expresar $Log(g)$, $\forall\, g \in (\mathbb{F}_{2^n})^*$ como una combinación lineal de los $Log(\pi_i)$.

[11] Considere parejas $(A, B) \in \mathbb{F}_2[x] \times \mathbb{F}_2[x]$ tales que $\deg(A) \leq n^{1/3}$, $\deg(B) \leq n^{1/3}$.

[12] Construya polinomios $(C, D) \in \mathbb{F}_2[x] \times \mathbb{F}_2[x]$ tales que:

$$C = Ax^h + B.$$

$$D = A^k x^{hk-n} f_1 + B^k.$$

[13] Se muestra fácilmente que

$$C^k \equiv D \pmod{f(X)}.$$

[14] Si C, D son b–suaves:

$$C = \prod_i \pi_i^{e_i}, \qquad D = \prod_i \pi_i^{f_i}.$$

[15]

$$\prod_i \pi_i^{ke_i} \equiv \prod_i \pi_i^{f_i} \pmod{f(x)}.$$

[16]

$$\sum_i (f_i - ke_i) Log(\pi_i) \equiv 0 \pmod{2^n - 1}.$$

[17] $\#(\mathbb{S})$ es grande, entonces

$$Log(z) = a_1 Log(\pi_1) + a_2 Log(\pi_2) + \ldots + a_s Log(\pi_s),\ \forall\ z \in (\mathbb{F}_{2^n})^*.$$

[18] Difícil escoger b, d.

Campos de funciones racionales: $\mathbb{F}_p(x)$

Conceptos y definiciones en el contexto de campos de funciones.

1. $\mathbb{F}_p(x) = \left\{ \frac{h(x)}{f(x)} \mid h(x), f(x) \in \mathbb{F}_p[x] \right\}$.
2. $p(x) \in \mathbb{F}_p[x]$ polinomio irreducible mónico.
3. Anillo de valuación asociado a $p(x)$:

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in \mathbb{F}_p[x],\ p(x) \not| g(x) \right\}.$$

4. Ideal maximal asociado a $p(x)$:

$$\wp_{p(x)} = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in \mathbb{F}_p[x],\ p(x) | f(x)\ p(x) \not| g(x) \right\}.$$

5.

$$\mathcal{O}_\infty = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in \mathbb{F}_p[x],\ \deg f(x) \leq \deg g(x) \right\}.$$

6. Primo infinito:

$$\wp_\infty = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in \mathbb{F}_p[x],\ \deg f(x) < \deg g(x) \right\}$$

7. Campo residual:

$$\Re_{P_{p(x)}} = \mathcal{O}_{p(x)}/P_{p(x)} \cong \mathbb{F}_p[x]/(p(x)).$$

8. Valuación discreta asociada al primo $P_{p(x)}$: $z \in \mathbb{F}_p(x) - 0$
$z = p(x)^n.(f(x)/g(x))$, $p(x) \not| f(x)$, $p(x) \not| g(x)$

$$\varphi_{P_{p(x)}}(z) = n.$$

9. Ceros y polos de $z \in \mathbb{F}_p(x) - 0$. $\varphi_{P_{p(x)}}(z) > 0$. $\varphi_{P_{p(x)}}(z) < 0$

10. Divisor principal asociado a $z \in \mathbb{F}_p(x) - 0$:

$$(z) = \prod \wp^{\varphi_\wp(z)} \prod \Omega^{\varphi_\Omega(z)}.$$

11. $\mathbb{F}_p$ es el campo de constantes de $\mathbb{F}_p(x)/\mathbb{F}_p$.

12. $\mathbb{P}(\mathbb{F}_p(x)) = \{P_{p(x)}, P_\infty | p(x) \text{ irreducible}\}$

13. Grado de un primo $P_{p(x)}$:

$$deg(P_{p(x)}) = [\Re_{P_{p(x)}} : \mathbb{F}_p].$$

14. $\wp \in \mathbb{P}(\mathbb{F}_p(x)/\mathbb{F}_p)$. $\wp$ es de grado 1 si y sólo si $\wp \in \mathbb{F}_p(x) \cup \{\infty\}$.

Campos de funciones en general:

Sea F/K campo de funciones, con K campo de constantes.

1. Grupo de divisores de F/K:

$$\mathcal{D}_F = < \wp | \wp \in \mathbb{P}(F) > .$$

$$\prod_\wp \wp^{\varphi_\wp}, \qquad \varphi_\wp == 0.$$

2. Grupo de divisores principales de F/K.

$$\mathcal{P}_F = \{(x) \mid 0 \neq x \in F\}.$$

3. Grupo de clases de F/K:

$$C_F = \mathcal{D}_F/\mathcal{P}_F.$$

4. Grupo de divisores de grado cero:

$$D_F^0 = \{A \in \mathcal{D}_F \mid \deg A = 0\}.$$

5. Grupo de clases de divisores de grado cero:

$$C_F^0 = \{[A] \in C_F \mid \deg[A] = 0\}.$$

6. Hecho: C_F^0 es grupo finito.

7. Número de clase de F/K:

$$h_F = \#(C_F^0).$$

Criba en campos de funciones (FFS): $\mathbb{F}_{p^n} \cong \frac{\mathbb{F}_p[x]}{<f>}$

1. Considere el campo finito $\mathbb{F}_{p^n} \cong \frac{\mathbb{F}_p[x]}{<f>}$.

2. f primitivo e irreducible de grado n.

$$\text{Grupo cíclico}: \ (\mathbb{F}_p[x]/f)^* =< x \pmod f > .$$

3. Cota de suavidad: $\sqrt{n}$, $\sqrt[2/3]{n}$.

4. Base de factores, consistente de polinomios:

$$\mathbb{S}_0 = \{h(x) \in \mathbb{F}_p[x] \mid \deg h(x) \leq \sqrt{n}\}.$$

Clave en FFS: Poder calcular:

$$Log_x(h), \quad \forall h \in \mathbb{S}_0.$$

Como calcular $Log_x(h)$?

(a) Tome $a \in \mathbb{N}$, $a < p^n - 1$.
Encuentre

$$x^a \pmod f$$

tal que $x^a \pmod f$ es $\sqrt{n}$–suave.

(b) Por $\sqrt{n}$–suavidad, obtendremos relaciones multiplicativas:

$$x^a \pmod f = \prod_{q_i \in \mathbb{S}} q_i^{e_i}.$$

(c) Buenas elecciones de $a'_s \rightarrow$ relaciones lineales entre $Log_x(q_i)$, $q_i \in \mathbb{S}_0$

$$a \equiv \sum_i e_i Log_x(q_i) \pmod{p^n - 1}.$$

(d) Cuantos a necesarios?

$$\#\mathbb{S}_0 + 1.$$

Como calcular $Log_x(g)$, $\quad g \in (\mathbb{F}_p[x]/f)^*$?

Bastará calcular:

$$Log_x(g), \qquad q \in \mathbb{S}, \forall q \in \mathbb{S}.$$

En efecto:

(a) Tome $a \in \mathbb{N}$, $a < p^n - 1$ tal que:

$$x^a g \pmod f \text{ es } \sqrt{n}\text{–suave en } \mathbb{S}.$$

Por tanto

$$x^a g = \prod_i q_i^{d_i}, \qquad q_i \in \mathbb{S}.$$

(b) De aquí que:

$$Log_x(g) \equiv -a + \sum_i d_i Log_x(q_i) \pmod{p^n - 1}, \quad q_i \in \mathbb{S}_0.$$

Optimizando el método del cálculo de indices

La base de factores usada es:

$$\mathbb{S}_0 = \{h(x) \text{ irreducibles } \in \mathbb{F}_p[x] \mid \deg h(x) \leq \sqrt{n}\}.$$

La base de factores que se usará, sera cuando la cota de suavidad es mas pequeña:

$$\mathbb{B} = \{h(x) \text{ irreducibles } \in \mathbb{F}_p[x] \mid \deg h(x) \leq \sqrt[3]{n}\}.$$

1. Formación de relaciones multiplicativas sobre la base de factores $\mathbb{S}$.
2. Solución al sistema lineal, obteniendo $Log_x(\pi_i), \pi_i \in \mathbb{S}$.

Dificultad para la formación de relaciones multiplicativas cuando la cota de suavidad es $\leq \sqrt[3]{n}$

En este caso, es complicado obtener las relaciones multiplicativas:

$$x^a \pmod f = \prod_{q_i \in \mathbb{S}} q_i^{e_i}.$$

Solución cuando la cota de suavidad es $\leq \sqrt[3]{n}$: Introducir un campo de funciones.

1. $m \in \mathbb{F}_p[x]$, $\deg m = n^{\frac{2}{3}}$.
2. $$H(x,y) \in \mathbb{F}_p[x,y], \qquad H(x,m) \equiv 0 \pmod f.$$
3. Como

   $H(x,m) \equiv 0 \pmod f$ se tiene la existencia de un homomorfismo :

   $$\phi : \begin{array}{ccc} \frac{\mathbb{F}_p[x,y]}{H} & \rightarrow & \frac{\mathbb{F}_p[x]}{f} \\ y & \rightarrow & m \end{array}.$$

4. Base de factores:

   $$\mathbb{S} = \{h(x) \text{ irreducibles } \in \mathbb{F}_p[x] \mid \deg h(x) \leq n^{1/3}\}.$$

5. Sea
$$C \text{ la curva definida por } H(x,y).$$

6. Campo de funciones de C sobre $\mathbb{F}_p$.
$$\mathbb{F}_p(C).$$

7. Relaciones multiplicativas sobre $\mathbb{S}$
Colección de parejas doblemente suaves:
Considere todos los primos relativos $r, s \in \mathbb{F}_p[x]$ donde $deg(r), deg(s) \leq c_3 n^{1/3} Log(n)^{2/3}$. Y tales que:
$(r,s) \in \mathbb{F}_p[x] \times \mathbb{F}_p[x]$, $ry + s \in \mathbb{F}_p(C)$.
(r,s) Doble Suave $\begin{cases} rm+s & \text{es } n^{1/3}\text{–suave} \\ r^d H(x, -s/r) & \text{es } n^{1/3}\text{–suave.} \end{cases}$

8. (r,s) Doble SUAVIDAD:
$$\boxed{\text{ry+s}} \xrightarrow{\phi} \boxed{\text{rm+s}}.$$

9. d: Grado de $H(x,y)$ en y
$$d = \lceil c_1^{-1} n^{1/3} Log^{-1/3}(n) Log^{1/3}(p) \rceil.$$

10.
$$d' = \lceil n/d \rceil, \qquad dd' = n + \delta$$
$$x^\delta f = m^d + a_{d-1} m^{d-1} + \ldots + a_0 \qquad a_i \in \mathbb{F}_p[x], \quad \deg(a_i) \leq d'.$$

11.
$$H = H_{m,f}(x,y) = y^d + a_{d-1} y^{d-1} + \ldots + a_0.$$

12. Sea $\wp$ primo de $\mathbb{F}_p(C)$.

13. Campo residual de $\wp$.
$$k_\wp := \mathcal{O}_\wp / \wp$$

14. Grado de $\wp$
$$d_\wp = [k_\wp : \mathbb{F}_p].$$

15. Asociando a cada primo $\wp$ un elemento del campo de funciones $\mathbb{F}_p(\mathcal{C})$:

$$\begin{array}{rccc} \alpha: & \mathbb{P}(\mathbb{F}_p(\mathcal{C})) & \rightarrow & \mathbb{F}_p(\mathcal{C}) \\ & \wp & \rightarrow & \alpha_\wp \end{array}$$

16. Sea $\mathcal{Q}$ primo de $\mathbb{F}_p(\mathcal{C})$ de grado 1.
El siguiente es un divisor de grado cero:

$$\left(\frac{\wp}{\mathcal{Q}}\right)^{d_\wp}.$$

17. Sea h el número de clase de $\mathbb{F}_p(\mathcal{C})$.

18. El siguiente es un divisor principal:

$$\left(\frac{\wp}{\mathcal{Q}}\right)^{hd_\wp} = \left(\alpha_\wp\right).$$

19. Considere el siguiente conjunto de primos:

$$\mathbb{S}' = \{\mathcal{Q} \in \mathbb{P}(\mathbb{F}_p(\mathcal{C})) \mid \mathcal{Q}/\mathcal{P}, \mathcal{P} \in \mathbb{S}\}.$$

20. Para cada pareja (r, s)–Doble suave calculamos $Div(ry + s)$, tenemos que:

$$Div(ry + s) = \prod_{\mathcal{Q}_i \in \mathbb{S}'} \mathcal{Q}_i^{a_i}.$$

21.

$$\deg\Big(Div(ry + s)\Big) = 0 = \sum_{i=1}^{z} a_i \deg(\mathcal{Q}_i).$$

22.

$$Div((ry + s)^h) = \prod_{\mathcal{Q}_i} \mathcal{Q}_i^{ha_i} =$$

$$\frac{\prod_{\mathcal{Q}_i} \mathcal{Q}_i^{ha_i}}{\prod_{\mathcal{Q}_i} \mathcal{Q}^{ha_i \deg(\mathcal{Q}_i)}} =$$

$$\left(\frac{\prod_{\mathcal{Q}_i} \mathcal{Q}_i^{h}}{\mathcal{Q}^{\sum_{\mathcal{Q}_i}^{h \deg(\mathcal{Q}_i)}}}\right)^{a_i} = \prod_{i=1}^{z} \alpha_i^{a_i}.$$

23.
$$(ry+s)^h = c\prod_{i=1}^{\#(\mathbb{S}')}\alpha_i^{a_i}, \qquad c\in\mathbb{F}_p^*.$$

24.
$$\phi(ry+s)\equiv rm+s \pmod f.$$

Como $rm+s$ es $\mathbb{S}$–suave, tenemos que:
$$rm+s=\prod_{g\in\mathbb{S}} g^{e_g}.$$

$$\prod_{g\in\mathbb{S}} g^{he_g}\equiv\phi(c)\prod_{i=1}^{\#(\mathbb{S}')}\phi(\alpha_i)^{a_i} \pmod f. \tag{1}$$

25. Logaritmos restringidos para $\alpha\in\mathbb{F}_{p^n}$ serán números $Log_*(\alpha)$ tales que:
$$Log_*(\alpha)$$
$$1\le Log_*(\alpha)\le\frac{p^n-1}{p-1}$$
$$\boxed{x^{Log_*(\alpha)}=\mu\alpha, \text{ para algun } \mu\in\mathbb{F}_p^*}.$$

Tomando logaritmos restringidos en (1), tenemos que:
$$\sum_{g\in\mathbb{S}} he_g Log_*(g)\equiv\sum_{i=1}^{\#(\mathbb{S}')} a_i Log_*(\phi(\alpha_i)) \pmod{\frac{p^n-1}{p-1}}.$$

26. El número de clase h se elige de tal forma que:
$$1=\left(h,\frac{p^n-1}{p-1}\right).$$

Calculando su inverso $\pmod{\frac{p^n-1}{p-1}}$ tenemos que:
$$h_1\equiv h^{-1} \pmod{\frac{p^n-1}{p-1}}.$$

27. Relaciones lineales entre $Log_*(g)$ y $Log_*(\phi(\alpha_i))$:

$$\sum_{g\in\mathbb{S}} e_g Log_*(g) \equiv \sum_{i=1}^{\#(\mathbb{S}')} a_i h_1 Log_*(\phi(\alpha_i)) \quad (\text{mód } \frac{p^n-1}{p-1}).$$

Habiendo coleccionado suficientes de tales relaciones, resolvemos para $Log_*(g), g \in \mathbb{S}$ y para $Log_*(\phi(\alpha_i))$.

28. Para cada $g \in \mathbb{S}$ calculamos $\mu \in \mathbb{F}_p$ tal que

$$x^{Log_*(g)} = \mu g.$$

29. Obteniendo:

$$Log_x(g) = Log_*(g) - Log_x(\mu).$$

30. Por Gordon, D (1993), Discrete Logaritms in $GF(p)$ using the number field sieve, obtenemos $Log_x(\mu), \forall \mu \in \mathbb{F}_p$.

31. Finalmente se obtiene $Log_x(g), \forall g \in \mathbb{S}$.

Referencias

[1] ADLEMAN L., MING-DEH, HUANG, A., *Function field sieve method for discrete logaritms over finite fields*, Information and Computation, (1909).

[2] BOREVICH AND SHAFAREVICH I., *Number Theory*, Academic Press, New York, (1966).

[3] COHEN H., *A Course in Computational Algebraic Number Theory*, Springer-Verlag, Berlin-Heidelberg-New York, 1996.

[4] HASSE, H., *Number Theory*, Springer-Verlag, (1978)

[5] HUNGERFORD, T., *Algebra* Springer-Verlag, (1974).

[6] KARPILOVSKY, G., *Topics in Field Theory*, North-Holland mathematics studies. **155**. The Netherlands (1992)

[7] KOBLITZ N., *A course in number theory y cryptography*, Springer-Verlag, Berlin-Heidelberg-New York, 1994.

[8] LANDAU, E., *Elementary Number Theory*, Chelsea Publishing Company, New York, (1958).

[9] LIDL, R., NIEDERREITER, H., *Finite Fields*, Encyclopedia of Mathematics y its Applications. Cambridge University Press. Vol 20, (1997)

[10] MARCUS, D., *Number Fields*, Springer, Universitext (1977).

[11] NARKIEWICZ, W., *Elementary y Analytic Theory of Algebraic Numbers*, Polish Scientific Publishers, (1974)

[12] Rose H. E., *A Course in Number Theory*, Clarendon Press, Oxford, 1994.

[13] ROSE, J., *A course on group theory*, Dover, (1994)

[14] STEPHEN, W., *The Mathematica book* Wolfram Media, Cambridge University Press (1999).

Sistemas Dinámicos y Sucesiones

Arturo Cueto Hernández
Universidad Autónoma Metropolitana–Azcapotzalco
Departamento de Ciencias Básicas
Av. San Pablo No. 180,
Col. Reynosa Tamaulipas
Azcapotzalco
02200 México, D.F.
arch@correo.azc.uam.mx

Resumen

Un problema que surge en el estudio de los sistemas dinámicos es determinar los conjuntos de puntos de período n, en particular la cardinalidad de estos; así, en forma natural tenemos asociado a un sistema dinámico una sucesión de enteros no negativos.

En este trabajo daremos una introducción al problema inverso, es decir, bajo que condiciones una sucesión de enteros no negativos representa la cardinalidad de los conjuntos de puntos de período n de un sistema. Finalmente presentamos una serie de propuestas de temas de tesis a nivel licenciatura.

1. Introducción

Un aspecto importante en muchas ramas de la matemática es el conocimiento del conjunto de puntos periódicos de un mapeo $T : \mathbb{X} \to \mathbb{X}$, donde tanto $\mathbb{X}$ y T poseerán algún tipo de estructura matemática. Por ejemplo, $\mathbb{X}$ puede ser un espacio topológico compacto y T un mapeo continuo, o $\mathbb{X}$ puede ser un grupo y T un automorfismo. La teoría ergódica y el estudio de los sistemas dinámicos proveen muchos ejemplos de estas categorías. Una pregunta natural se origina del estudio de este tipo de sistemas, ésta es acerca de las propiedades de sucesiones de enteros que cuentan el número de puntos periódicos.

2. Teoría Básica

En esta sección daremos algunas definiciones básicas respecto a los puntos periódicos de un mapeo y algunos ejemplos para motivar una serie de preguntas de carácter más general.

Definición 2.1.
Sea $\mathbb{X}$ *un conjunto no vacío y* $T : \mathbb{X} \to \mathbb{X}$ *un mapeo, el par* $(\mathbb{X}, T)$ *es un sistema.*

Definición 2.2.
El conjunto de puntos fijos del mapeo T *es*

$$Fix(T) = \{x \in \mathbb{X} : T(x) = x\}$$

Definición 2.3.
Para cada entero $n \geq 1$, *el conjunto de puntos periódicos de período* n *de* T *es*

$$Per_n(T) = Fix(T^n) = \{x \in \mathbb{X} : T^n(x) = x\}$$

Ejemplo 2.1.
Consideremos el mapeo $T : \mathbb{S}^1 \to \mathbb{S}^1$ dado por $T(z) = z^2$, donde $\mathbb{S}^1$ denota el círculo unitario. En la Figura 1. se muestra el único punto fijo de este mapeo, a saber $z = 1$.

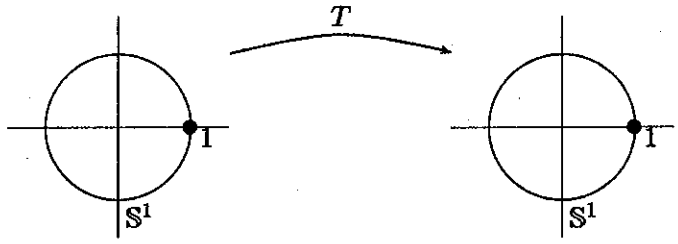


Figura 1. Punto fijo del mapeo $T(z) = z^2$.

Si $f_n = |Per_n(T)|$, $\{f_n\}$ es una sucesión de enteros no negativos. ¿Es $\{f_n\}$ una sucesión conocida?

Ejemplo 2.2.
Consideremos nuevamente el mapeo $T : \mathbb{S}^1 \to \mathbb{S}^1$ dado por $T(z) = z^2$. En la Figura 2. se muestra el único punto fijo de este mapeo, a saber $z = 1$. En la Figura 3. se muestran los puntos de período 2 y en la Figura 4. se muestran los puntos de período 3.

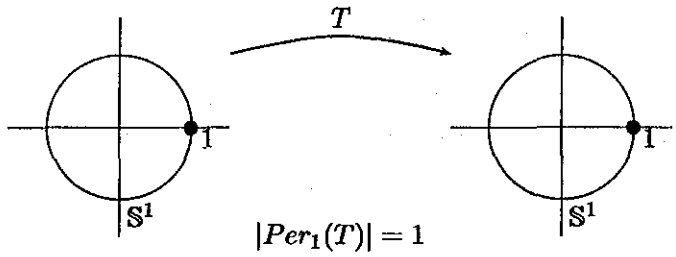


Figura 2. Puntos de período uno de $T(z) = z^2$.

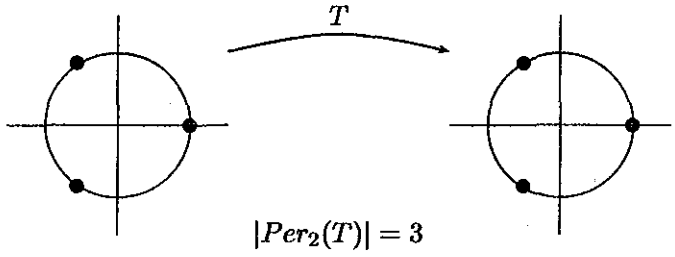


Figura 3. Puntos de período dos de $T(z) = z^2$.

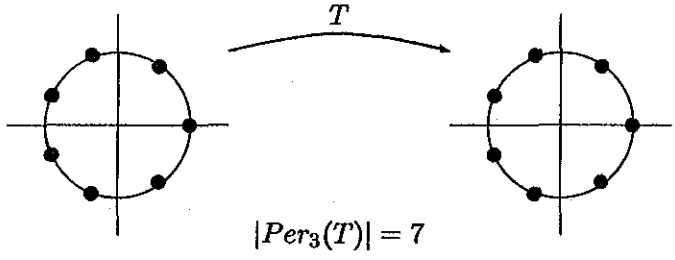


Figura 4. Puntos de período tres de $T(z) = z^2$.

Para determinar en general la cardinalidad del conjunto $Per_n(T)$, observemos que

$$|Per_n(T)| = |\{z \in \mathbb{S}^1 : z^{2^n} = z\}|$$

así debemos determinar el número de soluciones de

$$z^{2^n} - z = 0$$

que están en $\mathbb{S}^1$, éstas son las soluciones de

$$z^{2^n-1} - 1 = 0$$

por el teorema fundamental del álgebra tenemos

$$|Per_n(T)| = 2^n - 1$$

pero ésta es la expresión del n-ésimo número de Mersenne, es decir

$$f_n = M_n = \text{n-ésimo número de Mersenne}$$

Ejemplo 2.3.
La permutación $T = (1234)(56)$ actúa en el conjunto $\mathbb{X} = \{1, 2, 3, \ldots, 8\}$.

$$|Per_n(T)| = \begin{cases} 2 & , \ n \equiv 1 \pmod 4 \\ 4 & , \ n \equiv 2 \pmod 4 \\ 2 & , \ n \equiv 3 \pmod 4 \\ 8 & , \ n \equiv 0 \pmod 4 \end{cases}$$

$$\{f_n\} = \{|Per_n(T)|\} = \{2, 4, 2, 8, 2, 4, 2, 8, \ldots\}$$

Ejemplo 2.4.
Consideremos el grupo simétrico de orden 6,

$$S_3 = \langle a, b \, : \, a^3 = 1, \, b^2 = 1, \, a^b = a^{-1} \rangle$$

donde $a^b = b^{-1}ab$. Si $\varphi : S_3 \to S_3$ es el automorfismo interno,

$$\varphi : x \mapsto x^a, \ x \in S_3$$

$$|Per_n(\varphi)| = \begin{cases} 3 & , \ n \equiv 1 \pmod 3 \\ 3 & , \ n \equiv 2 \pmod 3 \\ 6 & , \ n \equiv 0 \pmod 3 \end{cases}$$

$$\{f_n\} = \{|Per_n(\varphi)|\} = \{3, 3, 6, 3, 3, 6, \ldots\}$$

Ejemplo 2.5.
Si $A = (a_{ij}) \in M_k(\{0,1\})$, $M_k(\{0,1\})$ matrices cuadradas de tamaño k con entradas 0 y 1, entonces si

$$\mathbb{X}_A = \{x \in \{0, 1, \ldots, k-1\}^{\mathbb{N}} \mid a_{x_j x_{j+1}} = 1 \text{ para todo } j \in \mathbb{N}\}$$

donde $\{0, 1, \ldots, k-1\}^{\mathbb{N}}$ denota el conjunto de todas las sucesiones en el conjunto $\{0, 1, \ldots, k-1\}$ y T_A es el desplazamiento a la izquierda del subconjunto cerrado $\mathbb{X}_A$ del espacio compacto $\{0, 1, \ldots, k-1\}^{\mathbb{N}}$, se tiene que $|Per_n(T_A)|$ depende de A.

Por ejemplo, si $\mathbb{X}_A = \{0, 1, \ldots, k-1\}^{\mathbb{N}}$ tenemos que

$$\{f_n\} = \{|Per_n(T_A)|\} = \{k, k^2, k^3, \ldots\}$$

Así, en el caso $k = 2$ tenemos que $\mathbb{X}_A$ es el conjunto de sucesiones de ceros y unos, y

$$\{f_n\} = \{|Per_n(T_A)|\} = \{2, 4, 8, \dots\}$$

Los primeros conjuntos de puntos periódicos bajo T_A son:

$$\begin{aligned}
Per_1(T_A) &= \{\{0,0,0,\dots\}, \{1,1,1,\dots\}\} \\
Per_2(T_A) &= \{\{0,0,0,\dots\}, \{1,1,1,\dots\}, \{0,1,0,1,0,1\dots\}, \\
&\quad \{1,0,1,0,1,0,\dots\}\} \\
Per_3(T_A) &= \{\{0,0,0,\dots\}, \{1,1,1,\dots\}, \{0,0,1,0,0,1,0,0,1\dots\}, \\
&\quad \{1,1,0,1,1,0,1,1,0,\dots\}, \{0,1,0,0,1,0,0,1,0,\dots\}, \\
&\quad \{1,0,1,1,0,1,1,0,1,\dots\}, \{1,0,0,1,0,0,1,0,0,\dots\}, \\
&\quad \{0,1,1,0,1,1,0,1,1,\dots\}\}
\end{aligned}$$

Ejemplo 2.6.
Sea $R = \mathbb{Z}\left[\frac{1}{q_1 \cdots q_s}\right]$ el subanillo más pequeño de los racionales en el cual los primos $q_1, \dots, q_s$ son invertibles. Entonces, para cada $\xi \in R^\times$, el automorfismo $T : \widehat{R} \to \widehat{R}$ dual al automorfismo $x \mapsto \xi x$ de R es un homeomorfismo de un espacio compacto con $\prod_{i=1}^{s} |\xi^n - 1|_{q_i} \times |\xi^n - 1|$ puntos de período n.

Por ejemplo, si $s = 1$, $q_1 = 2$, y $\xi = -2$, entonces esta construcción da un sistema $(\mathbb{X}, T)$ para el cual existen $|(-2)^n - 1|_2 \times |(-2)^n - 1| = |(-2)^n - 1|$ puntos de período n.

En estos ejemplos hemos visto como a sistemas específicos se asocian de manera natural sucesiones de enteros no negativos.

Problema Inverso

Dada una sucesión de enteros no negativos, $\{f_n\}$, ¿existirá un sistema $(\mathbb{X}, T)$ tal que $f_n = |Per_n(T)|$?

3. Sucesiones Realizables

En esta sección expondremos la teoría básicas de las sucesiones realizables y veremos como éstas permiten dar demostraciones más simples de resultados clásicos.

Definición 3.1.
Una sucesión $\{u_n\}$ *de enteros no negativos se dice realizable si existe un sistema* $(\mathbb{X}, T)$ *tal que para cada* $n \geq 1$, $u_n = |Per_n(T)|$.

Denotaremos el conjunto de todas las sucesiones realizables por $\mathcal{SR}$. Dada una clase de sucesiones de enteros no negativos $\mathcal{S}$, es natural preguntar: ¿qué es $\mathcal{S} \cap \mathcal{SR}$?. En este contexto planteamos los siguientes problemas:

Problema 3.1.
Si $\mathcal{S}$ es el conjunto de polinomios con coeficientes racionales, determine $\mathcal{S} \cap \mathcal{SR}$.

Problema 3.2.
Si $\mathcal{S}$ es el conjunto de todas las progresiones geométricas (de enteros no negativos), determine $\mathcal{S} \cap \mathcal{SR}$.

Problema 3.3.
Si $\mathcal{S}$ es el conjunto de todas las sucesiones que satisfacen una relación de recurrencia de segundo orden con coeficientes enteros y discriminante no cuadrado perfecto, determine $\mathcal{S} \cap \mathcal{SR}$.

Para resolver estos problemas es conveniente tener una caracterización de las sucesiones realizables; puesto que es sumamente complicado que dada una sucesión particular, aunque ésta sea realizable, dar un sistema con las propiedades requeridas. Para tal fin necesitaremos la función aritmética de Möbius.

Definición 3.2.
La función de Möbius está definida en los números naturales por

$$\mu(n) = \begin{cases} 1 & si\ n = 1 \\ 0 & si\ n\ no\ es\ libre\ de\ cuadrado \\ (-1)^r & si\ n\ es\ el\ producto\ de\ r\ primos\ distintos \end{cases}$$

Teorema 3.1. (Fórmula de Inversión de Möbius)
Sean f *y* g *sucesiones. Entonces* $f_n = \sum_{d|n} g_d$ *para cada* $n \geq 1$ *si y sólo si* $g_n = \sum_{d|n} \mu\left(\frac{n}{d}\right) f_d$ *para cada* $n \geq 1$.

Demostración:
Hardy–Wright [6, Teoremas 266 y 267]. □

Definición 3.3.
Una sucesión ϕ es multiplicativa si no es idénticamente cero y si

$$\phi(mn) = \phi(m)\phi(n)$$

para cada par m, n primos relativos.

Definición 3.4.
Una sucesión multiplicativa es completamente multiplicativa si

$$\phi(mn) = \phi(m)\phi(n)$$

para todo par m, n.

Teorema 3.2.
La función μ tiene las siguientes propiedades

(1) *μ es multiplicativa,*

(2) $\sum_{d|n} \mu(d) = 1$ *si* $n = 1$,

(3) $\sum_{d|n} \mu(d) = 0$ *si* $n > 1$,

(4) $\varphi(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) d$, *$\varphi$ es la función phi de Euler,*

(5) $\sum_{d|n} |\mu(d)| = 2^r$ *si* $n > 1$, *y r es el número de primos distintos que dividen a n.*

Demostración:
Hardy–Wright [6, Sección 16.3] □

Definición 3.5.
Dada una sucesión f sea

$$\widehat{f_n} = \sum_{d|n} \mu\left(\frac{n}{d}\right) f_d$$

para cada $n \geq 1$, y denotamos por $\widehat{f}$ la sucesión cuyo n-ésimo término es $\widehat{f_n}$.

Por la Fórmula de Inversión de Möbius tenemos

$$f_n = \sum_{d|n} \widehat{f_d}, \text{ para cada } n \geq 1 \tag{1}$$

3.1. Propiedades Elementales de los Puntos Periódicos

Sea $\mathbb{X}$ un conjunto y T un mapeo de $\mathbb{X}$ en $\mathbb{X}$. Sea $x \in \mathbb{X}$.

Definición 3.6.
Si n es un número natural tal que $T^n(x) = x$, entonces x se dice que es periódico y que tiene período n.

Definición 3.7.
Si x es periódico, entonces el período mínimo de x es el mínimo número natural n para el cual $T^n(x) = x$.

Definición 3.8.
La órbita O_x de x es el conjunto $\{T^s(x) : s \in \mathbb{Z}^+\}$.

Definición 3.9.
Para cada $n \geq 1$, sean

$$F_n = \{x \in \mathbb{X} : x \text{ tiene período } n\},$$

$$G_n = \{x \in \mathbb{X} : x \text{ tiene período mínimo } n\}$$

Lema 3.1.
Supóngase que n es un número natural y $x \in \mathbb{X}$. Lo siguiente se tiene:

(i) *Si $x \in F_n$, entonces el período mínimo de x divide a n,*

(ii) *Si $x \in G_n$, entonces $O_x = \{x, T(x), \ldots, T^{n-1}(x)\}$,*

(iii) $F_n = \bigcup_{d|n} G_d$, *la unión es disjunta,*

(iv) *Si $x \in G_n$, entonces $O_x \subseteq G_n$,*

(v) *Si $x \in G_n$, entonces $|O_x| = n$,*

(vi) *Si G_n es un conjunto finito, entonces $n||G_n|$.*

Demostración:
(i) Sea x tal que tiene período n. Supongamos que l es el período mínimo de x y, por el algoritmo de la división, sean $m, k \in \mathbb{Z}^+$ tales que $n = k + lm$ con $k < l$. Entonces

$$x = T^n(x) = T^{k+lm}(x) = T^k[(T^l)^m(x)] = T^k(x).$$

Así tenemos que $x = T^k(x)$. Por otra parte, $k < l$ y l es el período mínimo de x. Por lo tanto, $k = 0$ y $n = lm$.

(ii) Sea x tal que tiene período mínimo n. Por la Definición 3.8

$$\{x, T(x), \ldots, T^{n-1}(x)\}$$

es un subconjunto de O_x.

Veamos que O_x es un subconjunto de $\{x, T(x), \ldots, T^{n-1}(x)\}$, supongamos que $T^z(x) \in O_x$ para algún $z \in \mathbb{Z}^+$. Sean $m, k \in \mathbb{Z}^+$ tales que $z = k+nm$ con $k < n$. Así, $T^k(x)$ está en $\{x, T(x), \ldots, T^{n-1}(x)\}$. Pero,

$$T^z(x) = T^k[(T^n)^m(x)] = T^k(x)$$

puesto que x tiene período n.

(iii) La unión es disjunta dado que cada punto en $\mathbb{X}$ tiene a lo más un período mínimo. La unión es un subconjunto de F_n porque si $d|n$ y $T^d(x) = x$ para algún $x \in \mathbb{X}$, entonces

$$T^n(x) = (T^d)^{n/d}(x) = x.$$

Por otra parte, F_n es un subconjunto de la unión porque si $T^n(x) = x$ para algún $x \in \mathbb{X}$, entonces x tiene un período mínimo el cual, por (i), es un divisor de n.

(iv) Sea x tal que tiene período mínimo n. Tomemos cualquier $k \in \{0, 1, \ldots, n-1\}$. Por (ii), basta con demostrar que $T^k(x)$ tiene período n. Tenemos

$$T^n[T^k(x)] = T^k[T^n(x)] = T^k(x)$$

puesto que n es un período de x. Así, n es un período de $T^k(x)$. Sea $l \leq n$ el período mínimo de $T^k(x)$. De esta manera, $T^l[T^k(x)] = T^k(x)$ y, por lo tanto,

$$T^{n-k}(T^l[T^k(x)]) = T^{n-k}[T^k(x)].$$

De donde, $T^l[T^n(x)] = T^n(x)$ y, como n es un período de x, tenemos

$$T^l(x) = x.$$

Pero n es el período mínimo de x. Por lo tanto, $n \leq l$. Pero como hemos elegido $l \leq n$, se sigue que $l = n$. Así, n es el período mínimo de $T^k(x)$.

(v) Sea x tal que tiene período mínimo n. Por (ii), basta con demostrar que los elementos de $\{x, T(x), \ldots, T^{n-1}(x)\}$ son distintos. Supongamos lo

contrario, es decir, $T^i(x) = T^j(x)$ para algunos i y j con

$$0 \leq i < j < n \tag{2}$$

Entonces, $T^{n-i}[T^i(x)] = T^{n-i}[T^j(x)]$, lo cual implica que

$$T^n(x) = T^{j-i}[T^n(x)].$$

Como n es un período de x, tenemos $x = T^{j-i}(x)$. Por (2) tenemos que $j - i$ es positivo y, dado que n es el período mínimo de x, tenemos $j - i \geq n$. Así, $j \geq n$. Pero por (2) $j < n$. Esta contradicción prueba (v).

(vi) Definamos una relación $\sim$ en G_n como sigue. Para cada par x y y en G_n decimos que $x \sim y$ si y sólo si $x \in O_y$. Veamos que $\sim$ es una relación de equivalencia, sean w, x y y en G_n. Ésta es reflexiva puesto que $x \in O_x$ (Definición 3.8). Ésta es transitiva porque si $z_1, z_2 \in \mathbb{Z}^+$ con $w = T^{z_1}(x)$ y $x = T^{z_2}(y)$, entonces $w = T^{z_1+z_2}(y)$. Ahora demostremos la simetría, sea $x \in O_y$. Por (ii), escojamos un r tal que $0 \leq r < n$ y $x = T^r(y)$. Entonces

$$T^{n-r}(x) = T^{n-r}[T^r(y)] = T^n(y) = y$$

ya que n es un período de y. Así, $y \in O_x$, demostrando que $\sim$ es simétrica. Por lo tanto, $\sim$ es una relación de equivalencia en G_n.

Para cada $x \in G_n$ la clase de equivalencia de x es $\{y \in G_n \mid y \in O_x\}$. Ésta es igual a O_x por (iv). También tenemos $\#O_x = n$ por (v). Así, si G_n es un conjunto finito, entonces $n \mid \#G_n$. □

Lema 3.2. Lema Básico
Sea f una sucesión de enteros no negativos. Entonces f es realizable si y sólo si para cada $n \geq 1$

(i) *$\widehat{f}_n$ es un entero no negativo,*

(ii) *n divide a $\widehat{f}_n$.*

Demostración:
Demostraremos por el momento la parte del *sólo si*. Sea $(\mathbb{X}, T)$ un sistema tal que $f_n = |F_n|$ para cada $n \geq 1$. Como f es una sucesión en $\mathbb{Z}^+$, lo mismo se tiene para la sucesión $\{|G_n|\}$ ya que $G_n \subseteq F_n$. Por lo tanto

$$f_n = \sum_{d|n} |G_d|$$

Luego

$$|G_n| = \sum_{d|n} \mu\left(\frac{n}{d}\right) f_d = \widehat{f}_n$$

Esto prueba que $\widehat{f}_n$ es un entero no negativo, ya que $\{|G_n|\}$ es una sucesión en $\mathbb{Z}^+$.

Por (vi) del Lema anterior se sigue que n divide a $\widehat{f}_n$. □

Para el recíproco, demostraremos un enunciado más fuerte en el sentido que exhibiremos un sistema en el cual el mapeo T es un homeomorfismo de un espacio compacto.

Definición 3.10.
Un sistema dinámico es un triada $(\mathbb{X}, \tau, T)$ donde $(\mathbb{X}, \tau)$ es un espacio topológico compacto y $T : \mathbb{X} \to \mathbb{X}$ es un homeomorfismo of $(\mathbb{X}, \tau)$.

Definición 3.11.
Dada una sucesión f, decimos que f es realizable por un sistema dinámico si existe un sistema dinámico $(\mathbb{X}, \tau, T)$ tal que el sistema $(\mathbb{X}, T)$ realiza a f.

Lema 3.3.
Si f es una sucesión con $\widehat{f}_n \in \mathbb{Z}^+$ y $n|\widehat{f}_n$ para cada $n \geq 1$, entonces f es realizable por un sistema dinámico.

En la demostración del Lema 3.3 usaremos la noción de compactificación, por tal motivo daremos la definición de ésta y un ejemplo para fijar las ideas.

Definición 3.12.
Sean $(\mathbb{X}_*, \tau_*)$ y $(\mathbb{X}, \tau)$ espacios topológicos. Entonces $(\mathbb{X}_*, \tau_*)$ es una compactificación de $(\mathbb{X}, \tau)$ si $(\mathbb{X}_*, \tau_*)$ es compacto y contiene a un subespacio denso homeomorfo a $(\mathbb{X}, \tau)$.

Ejemplo 3.1. Sea $(\mathbb{X}, \tau)$ un espacio no compacto. Por ejemplo, $(\mathbb{N}, 2^{\mathbb{N}})$, el espacio de los números naturales con la topología discreta. Sea I un conjunto no vació el cual no interseca a $\mathbb{X}$, tomando la unión de éste con $\mathbb{X}$ formamos el conjunto $\mathbb{X}_* = \mathbb{X} \cup I$. Definimos τ_* como la colección de todos los conjuntos de los siguientes tipos:

(I) U, donde U está en τ;

(II) $U \cup I$, donde U está en τ y $\mathbb{X} - U$ es compacto en $(\mathbb{X}, \tau)$.

Se puede demostrar que τ_* es una topología para $\mathbb{X}_*$, que $(\mathbb{X}_*, \tau_*)$ es compacto y que $(\mathbb{X}, \tau)$ es un subespacio denso de $(\mathbb{X}_*, \tau_*)$. Para el caso cuando I es un conjunto de un elemento, la demostración puede verse, por ejemplo, en las demostraciones de las Proposiciones 5.21 y 5.22 de Cain [3]. Estas demostraciones, con algunos cambios, también demuestran el caso general. Así, $(\mathbb{X}_*, \tau_*)$ es una compactificación de $(\mathbb{X}, \tau)$. Cuando I es un conjunto de un elemento es usual escribir $I = \{\infty\}$ y la compactificación se llama compactificación de Alexandroff o compactificación en un punto. Se llamará compactificación en k puntos cuando $I = \{\infty_1, \ldots, \infty_k\}$.

Demostración (Lema 3.3):
Sea f una sucesión con $\widehat{f}_n \in \mathbb{Z}^+$ y $n|\widehat{f}_n$ para cada $n \geq 1$. Para cada $n \geq 1$, sea $s_n := \sum_{i=1}^{n} \widehat{f}_i$. Existen cuatro casos:

(i) $\widehat{f}$ tiene un término positivo y eventualmente es cero;

(ii) $\widehat{f}_1$ es positivo y $\widehat{f}$ no es eventualmente cero;

(iii) $\widehat{f}_1$ es 0 y $\widehat{f}$ no es eventualmente cero;

(iv) $\widehat{f}$ es la sucesión de ceros.

Para el caso (i), supongamos que $\widehat{f}_l$ es el último término positivo de $\widehat{f}$. Sea $\mathbb{X} = \{1, 2, \ldots, s_l\}$ y definamos $T : \mathbb{X} \to \mathbb{X}$ como el producto de los siguientes ciclos:

$\widehat{f}_1$ ciclos de longitud 1 $(1)(2)\ldots(s_1)$;
$\widehat{f}_2/2$ ciclos de longitud 2 $(s_1+1, s_1+2)(s_1+3, s_1+4)\ldots(s_2-1, s_2)$;
$\widehat{f}_3/3$ ciclos de longitud 3 $(s_2+1, s_2+2, s_2+3)\ldots(s_3-2, s_3-1, s_3)$;

y así hasta terminar con los $\widehat{f}_l/l$ ciclos de longitud l:

$$(s_{l-1}+1, s_{l-1}+2, \ldots, s_{l-1}+l)\ldots(s_l-l+1, \ldots, s_l-1, s_l)$$

T es una biyección bien definida puesto que cada elemento de $\mathbb{X}$ aparece en exactamente un ciclo. Dotando a $\mathbb{X}$ de la topología discreta se obtiene el espacio $(\mathbb{X}, 2^{\mathbb{X}})$, así se tiene que T es un homeomorfismo. Este espacio es compacto dado que $\mathbb{X}$ es finito. Por lo tanto, $(\mathbb{X}, 2^{\mathbb{X}}, T)$ es un sistema dinámico.

Ahora demostraremos que, para cada $n \geq 1$, el número de puntos de período n es igual a f_n. En la definición de T, para cada n existen $\widehat{f}_n/n$

ciclos de longitud n. Por lo tanto, G_n es un conjunto finito para cada n, y $\#G_n = \widehat{f}_n$. Luego, usando (1) y el Lema 3.1(iii), para cada $n \geq 1$,

$$f_n = \sum_{d|n} \widehat{f}_d = \sum_{d|n} \#G_d = \#F_n.$$

Así, f es realizable en el caso (i).

Para (ii), sea $(\mathbb{N}_*, 2^{\mathbb{N}}_*)$ la compactificación en un punto de $(\mathbb{N}, 2^{\mathbb{N}})$. Es decir, $\mathbb{N}_* = \mathbb{N} \cup \{\infty\}$. Definamos el mapeo $T : \mathbb{N}_* \to \mathbb{N}_*$ como el producto de los ciclos siguientes:

$$\underbrace{(\infty)(1)(2)\dots(s_1-1)}_{\widehat{f}_1 \text{ ciclos de longitud } 1} \quad \underbrace{(s_1, s_1+1)\dots(s_2-2, s_2-1)}_{\widehat{f}_2/2 \text{ ciclos de longitud } 2}$$

$$\underbrace{(s_2, s_2+1, s_2+2)\dots(s_3-3, s_3-2, s_3-1)}_{\widehat{f}_3/3 \text{ ciclos de longitud } 3}$$

y así sucesivamente. En esta definición de T, si $s_1 = 1$, entonces se supone que el ciclo de longitud 1 es (∞). Tenemos que $(\mathbb{N}_*, 2^{\mathbb{N}}_*)$ es compacto. Por las mismas razones dadas en el caso (i), T es una biyección y $f_n = \#F_n$ para cada $n \geq 1$. Por lo tanto, será suficiente con demostrar que T y T^{-1} mandan elementos de $2^{\mathbb{N}}_*$ a elementos de $2^{\mathbb{N}}_*$.

Recordemos que los conjuntos abiertos son de los tipos (I) y (II) de acuerdo al Ejemplo 3.1. Sea $U \in 2^{\mathbb{N}}_*$ del tipo (I). Entonces, U es un subconjunto de $\mathbb{N}$. Por la definición de T, $T(U)$ también es un subconjunto de $\mathbb{N}$. Por lo tanto, $T(U)$ está en $2^{\mathbb{N}}$ y en consecuencia es del tipo (I). Así, $T(U) \in 2^{\mathbb{N}}_*$.

Para los conjuntos abiertos del tipo (II), notemos que, como en cualquier espacio discreto, los conjuntos compactos en $(\mathbb{N}, 2^{\mathbb{N}})$ son los subconjuntos finitos de $\mathbb{N}$. Sea $U \cup I$ del tipo (II), así que U es un subconjunto de $\mathbb{N}$ y $\mathbb{N} - U$ es finito. Tenemos

$$T(U \cup I) = T(U) \cup T(I) = T(U) \cup I,$$

lo cual se demostrará que está en $2^{\mathbb{N}}_*$. De hecho, $T(U) \cup I$ es un conjunto de tipo (II) por las siguientes razones: $T(U)$ es un subconjunto de $\mathbb{N}$ y, por lo tanto, está en $2^{\mathbb{N}}$; también, $\mathbb{N} - T(U)$ es finito puesto que $\mathbb{N} - U$ es finito y $T(\mathbb{N} - U) = T(\mathbb{N}) - T(U) = \mathbb{N} - T(U)$; luego, $\mathbb{N} - T(U)$ es compacto en $(\mathbb{N}, 2^{\mathbb{N}})$. Así, $T(U) \cup I$ está en $2^{\mathbb{N}}_*$. Hemos demostrado que T manda conjuntos abiertos en conjuntos abiertos. Por las misma razones, lo mismo se tiene para

T^{-1}. Por lo tanto, $(\mathbb{N}_*, 2^{\mathbb{N}}_*, T)$ es un sistema dinámico que realiza a f, lo cual establece el caso (ii).

Para (iii), sea $k > 1$ tal que $\widehat{f}_1 = \cdots = \widehat{f}_{k-1} = 0$ y $\widehat{f}_k \neq 0$. Sea $(\mathbb{N}_*, 2^{\mathbb{N}}_*)$ la compactificación en $\widehat{f}_k$ puntos de $(\mathbb{N}, 2^{\mathbb{N}})$. Es decir, $\mathbb{N}_* = \mathbb{N} \cup \{\infty_1, \ldots, \infty_{\widehat{f}_k}\}$. Definamos el mapeo $T : \mathbb{N}_* \to \mathbb{N}_*$ como el producto de los ciclos siguientes:

$$\underbrace{(\infty_1, \ldots, \infty_k) \ldots (\infty_{\widehat{f}_k - k+1}, \ldots, \infty_{\widehat{f}_k})}_{\widehat{f}_k/k \text{ ciclos de longitud } k}$$

$$\underbrace{(1, 2, \ldots, k+1) \ldots (\widehat{f}_{k+1} - k, \ldots, \widehat{f}_{k+1})}_{\widehat{f}_{k+1}/(k+1) \text{ ciclos de longitud } k+1}$$

siguiendo con los $\widehat{f}_{k+2}/(k+2)$ ciclos disjuntos cada uno de longitud $k+2$ usando los números $\widehat{f}_{k+1} + 1, \ldots, \widehat{f}_{k+1} + \widehat{f}_{k+2}$, y así sucesivamente. Usando el mismo argumento que en el caso (ii), f es realizable por $(\mathbb{N}_*, 2^{\mathbb{N}}_*, T)$.

Finalmente, para el caso (iv) sea $\widehat{f} = 0$. Así, $f = 0$ por (1). De acuerdo al Lema 3.1(iii), debemos dar un sistema dinámico para el cual $\#G_n = 0$ para cada $n \geq 1$. Por el Lema 3.1(v), esto será realizado si damos un sistema dinámico en el cual ninguna órbita es finita: sea α un irracional; consideremos el espacio métrico compacto $(\mathbb{S}^1, \rho)$, donde $\mathbb{S}^1 = \{\omega \in \mathbb{C} \mid |\omega| = 1\}$ y ρ es la métrica usual en $\mathbb{C}$; definamos el homeomorfismo T de $(\mathbb{S}^1, \rho)$ dado por $T(\omega) = \omega e^{2\pi i \alpha}$ para cada $\omega \in \mathbb{S}^1$; el Teorema de Jacobi establece que la órbita de cada punto de $\mathbb{S}^1$ es densa en $(\mathbb{S}^1, \rho)$. Así, $(\mathbb{S}^1, \rho, T)$ es un sistema dinámico que realiza a f.

Esto concluye la demostración del Lema 3.3 y, por lo tanto, también la del Lema Básico. □

Proposición 3.1.
Si f, g son sucesiones realizables y $fg = 0$, entonces $f = 0$ o $g = 0$.

Demostración:
Demostraremos algo más general: si f y g son sucesiones en $\mathbb{R}$ con $\widehat{f}, \widehat{g} \geq 0$ y $fg = 0$, entonces $f = 0$ o $g = 0$. La proposición se sigue inmediatamente del Lema Básico.

Sean f, g en $\mathbb{R}$ con $\widehat{f}, \widehat{g} \geq 0$ y $fg = 0$. Así, $f, g \geq 0$ por (1). Supongamos que ninguna de las dos f y g es idénticamente cero. Sean k, l tales que

$f_k, g_l > 0$. Como $\widehat{f} \geq 0$, se sigue de (1) que

$$f_{kl} = \sum_{d|kl} \widehat{f}_d \geq \sum_{d|k} \widehat{f}_d = f_k.$$

Similarmente, $g_{kl} \geq g_l$. Por lo tanto, $f_{kl} g_{kl} \geq f_k g_l > 0$. Esto contradice que $fg = 0$. □

Proposición 3.2.
Una sucesión constante en $\mathbb{Z}^+$ es realizable.

Demostración:
Sean $s \in \mathbb{Z}^+$ y f la sucesión constante $\{s\}$. Tenemos

$$\widehat{f}_n = \sum_{d|n} \mu\left(\frac{n}{d}\right) f_d = \sum_{d|n} \mu\left(\frac{n}{d}\right) s = s \sum_{d|n} \mu\left(\frac{n}{d}\right)$$

el cual es igual a s cuando $n = 1$, y 0 en otro caso. Así, por el Lema Básico f es realizable. □

Proposición 3.3.
Si f es una sucesión realizable, entonces también lo es sf para cada $s \in \mathbb{Z}^+$.

Demostración:

$$\left(\widehat{sf}\right)_n = \sum_{d|n} s f_d \mu\left(\frac{n}{d}\right) = s \sum_{d|n} f_d \mu\left(\frac{n}{d}\right) = s\widehat{f}_n$$

□

Proposición 3.4.
Si a es un entero positivo entonces la sucesión $\{a^n\}_{n\geq 1}$ es realizable.

Demostración:
Sea $\mathbb{X}$ el conjunto de sucesiones $\{0, 1, \ldots, a-1\}^{\mathbb{N}}$ y sea $T : \mathbb{X} \to \mathbb{X}$ el mapeo desplazamiento a la izquierda, es decir, si $x = (x_1, x_2, x_3, \ldots) \in \mathbb{X}$ entonces

$$T(x) = (x_2, x_3, x_4, \ldots)$$

Entonces se puede ver que el sistema $(\mathbb{X}, T)$ realiza a la sucesión $\{a^n\}_{n\geq 1}$. □

Teorema 3.3. (Teorema de Euler–Fermat)
Si $n > 1$ y $(a, n) = 1$ entonces

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

donde φ es la función phi de Euler.

En demostraciones estándares de este Teorema (Hardy–Wright [6, Sección 6.3]) primero se demuestra que

$$a^{p^r} \equiv a^{p^{r-1}} \pmod{p^r} \quad \forall\, a \in \mathbb{Z},\ r \in \mathbb{N} \text{ y } p \text{ primo.}$$

El Teorema entonces se sigue inmediatamente de algunas propiedades básicas de congruencias y del hecho de que φ es multiplicativa.

Demostración:
Únicamente estableceremos la validez de la congruencia

$$a^{p^r} \equiv a^{p^{r-1}} \pmod{p^r} \quad \forall\, a \in \mathbb{Z},\ r \in \mathbb{N} \text{ y } p \text{ primo.}$$

La congruencia anterior se tiene inmediatamente para $a = 0$ y $a = -1$. Para $a < -1$ la congruencia se obtiene de la congruencia para $a > 1$. Así, sea $a \in \mathbb{N}$, entonces la sucesión $\{a^n\}$ es realizable. Luego, el p^r–ésimo término de $\{\widehat{a^n}\}$ es

$$a^{p^r} - a^{p^{r-1}}$$

el cual es divisible por p^r. □

3.2. Positividad y Divisibilidad

Definición 3.13.
Una sucesión $\{x_n\}$ de reales no negativos tiene positividad si $\widehat{x}_n \geq 0$ para cada $n \geq 1$.

Definición 3.14.
Una sucesión $\{x_n\}$ de enteros tiene divisibilidad si $n|\widehat{x}_n$ para cada $n \geq 1$.

Comentario 3.1.
El Lema Básico establece que una sucesión es realizable si y sólo si tiene positividad y divisibilidad.

Proposición 3.5.
Sean p un número primo y $u = \{u_n\}$ una sucesión de enteros no negativos. Si u es una sucesión realizable entonces

$$u_p - u_1 \geq 0 \quad y \quad p|u_p - u_1.$$

Demostración:
Directa de las definiciones y el Comentario 3.1. □

3.3. Sucesiones Tipo Fibonacci

Definición 3.15.
Una sucesión f es tipo Fibonacci si

$$f_{n+2} = f_{n+1} + f_n \text{ para cada } n \geq 1 \tag{3}$$

La sucesión de Fibonacci se tiene con $F_1 = 0$ y $F_2 = 1$.

La sucesión de Lucas se tiene con $L_1 = 1$ y $L_2 = 3$.

$$F = \{0, 1, 1, 2, 3, 5, \dots\} \text{ y } L = \{1, 3, 4, 7, 11, 18, \dots\}$$

Proposición 3.6.
Si f es tipo Fibonacci, entonces

$$f_n = f_1 F_{n-1} + f_2 F_n \text{ para cada } n \geq 2. \tag{4}$$

Demostración:
Por inducción. Sea f una sucesión tipo Fibonacci. Entonces para $n = 2$, tenemos:

$$f_2 = f_1 F_1 + f_2 F_2 = f_1 \cdot 0 + f_2 \cdot 1 = f_2$$

así la fórmula es válida para $n = 2$. Supongamos que la fórmula es válida hasta $n = k$, es decir,

$$f_j = f_1 F_{j-1} + f_2 F_j \quad 2 \leq j \leq k$$

Entonces para $n = k + 1$, tenemos:

$$\begin{aligned} f_{k+1} &= f_k + f_{k-1} \\ &= f_1 F_{k-1} + f_2 F_k + f_1 F_{k-2} + f_2 F_{k-1} \\ &= f_1(F_{k-1} + F_{k-2}) + f_2(F_k + F_{k-1}) \\ &= f_1 F_k + f_2 F_{k+1} \end{aligned}$$

Por lo tanto, la fórmula es válida para todo n. □

Teorema 3.4.
Sea f tipo Fibonacci con $f_1 \in \mathbb{Z}^+$. Entonces f es realizable si y sólo si $f_2 = 3f_1$.

Demostración:
Sea $f_2 = 3f_1$. Entonces $f = f_1\{1, 3, 4, 7, \dots\} = f_1 L$. Basta con demostrar que L es realizable. Para esto utilizaremos la siguiente proposición:

Proposición 3.7.
Para toda matriz cuadrada A con entradas enteras no negativas, $A \in M_k(\mathbb{Z}^+)$, existe un sistema $(\mathbb{X}_A, T_A)$ el cual tiene exactamente $\mathrm{tr}(A^n)$ *puntos de período n.*

Demostración:
Lind–Marcus [8]. □

Sean

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad , \quad A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

y $t_n = \mathrm{tr}(A^n)$ para cada $n \geq 1$. Tenemos que el polinomio característico de A es $x^2 = x + 1$. Por lo tanto, $A^2 = A + I$. De donde, $A^{n+2} = A^{n+1} + A^n$, y en consecuencia

$$t_{n+2} = t_{n+1} + t_n \text{ para cada } n \geq 1.$$

Así, t y L satisfacen la misma relación de recurrencia. Además,

$$\begin{aligned} t_1 &= 1 + 0 = 1 = L_1 \\ t_2 &= \mathrm{tr}(A^2) = \mathrm{tr}(A + I) \\ &= \mathrm{tr}(A) + \mathrm{tr}(I) = 1 + 2 = 3 = L_2 \end{aligned}$$

Por lo tanto, $t = L$. Así, L es realizable.

Recíprocamente, supóngase que f es realizable. Sea p un número primo. Entonces

$$p | \widehat{f_p} = f_p - f_1$$

De donde, por (4),

$$f_1(F_{p-1} - 1) + f_2 F_p \equiv 0 \pmod{p}$$

Esta congruencia se cumple con $f_1 = 1$ y $f_2 = 3$, hemos demostrado que la sucesión de Lucas es realizable. Así,

$$F_{p-1} - 1 + 3F_p \equiv 0 \pmod{p} \tag{5}$$

Si

$$F_p \equiv 1 \pmod{p} \text{ para cada } p \equiv 2 \pmod{5} \tag{6}$$

entonces para $p \equiv 2 \pmod{5}$ tenemos

$$F_{p-1} \equiv -2 \pmod{p}$$

así obtenemos

$$f_2 \equiv 3f_1 \pmod{p}$$

Por lo tanto, el resultado se tiene ya que 2 y 5 son primos relativos, por el Teorema de Dirichlet existe una infinidad de p tales que $p \equiv 2 \pmod 5$.

Por último, justificaremos la congruencia (6). Sea $p \equiv 2 \pmod 5$. Entonces, por (Hardy–Wright [6, Teorema 180])

$$F_{p+2} \equiv 0 \pmod{p}$$

De la relación de Fibonacci (3) se tiene

$$F_{p+2} = 2F_p + F_{p-1}$$

Así, $2F_p + F_{p-1} \equiv 0 \pmod p$, restando ésta de (5), obtenemos

$$F_p \equiv 1 \pmod{p} \text{ para cada } p \equiv 2 \pmod 5$$

□

Comentario 3.2. *La congruencia* (5) *es una de las formas en que la sucesión de Fibonacci puede ser rápidamente obtenida. Cómo la sucesión de Lucas, L, es realizable, la condición (ii) del Lema Básico implica:*

$$\sum_{d|n} \mu(n/d)L_d \equiv 0 \pmod{n} \quad \textit{para cada } n \geq 1.$$

Por lo tanto, si $n = p^r$ donde p es un número primo y $r \geq 1$ se obtiene

$$L_{p^r} \equiv L_{p^{r-1}} \pmod{p}^r,$$

o bien, si $n = pq$ donde p y q son números primos distintos se obtiene

$$L_{pq} + 1 \equiv L_p + L_q \pmod{pq},$$

y así sucesivamente. Es probable que tales congruencias sean conocidas. Sin embargo, ellas no son triviales.

Comentario 3.3. *Es conveniente que tengamos un sistema que realiza a la sucesión de Lucas, L. Ya que, para demostrar que L es realizable de acuerdo al Lema Básico, tendríamos que verificar directamente que $\widehat{L} \geq 0$ y que $n|\widehat{L}_n$ para cada $n \geq 1$. Es relativamente fácil demostrar que $\widehat{L} \geq 0$. Sin embargo, es difícil ver como demostrar directamente que $n|\widehat{L}_n$ para cada $n \geq 1$. La sucesión de Lucas pertenece a una clase de sucesiones que generan tal dificultad.*

Comentario 3.4. *El Teorema* 3.4 *trata de la realización de un tipo particular de sucesiones que satisfacen una relación de recurrencia de segundo orden lineal, queda pendiente hacer un estudio general de la realización de las sucesiones que satisfacen una relación de recurrencia de segundo orden lineal con coeficientes enteros. En esta dirección seguiría un estudio de la realización de sucesiones de tercer orden o mayor, desde luego este estudio es más difícil, pero una pregunta básica y natural en el "espíritu de Fibonacci" sería como sigue: Sea* $r \in \mathbb{N}$. *Definimos una sucesión* f *como* r*–Fibonacci si*

$$f_{n+r} = f_{n+r-1} + f_{n+r-2} + \cdots + f_n \quad \text{para cada } n \geq 1. \tag{7}$$

Definamos la sucesión r*–Lucas,* $L^{(r)}$, *como la sucesión que satisface esta recurrencia y* $L_n^{(r)} = 2^n - 1$ *para cada* $1 \leq n \leq r$. *De este modo,* $L^{(1)}$ *es la sucesión de unos y* $L^{(2)}$ *es la sucesión de Lucas clásica,* L. *Sea*

$$A_r = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ & & \ddots & & & \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{bmatrix}$$

una matriz de tamaño r *de ceros y unos, es decir,* $A_r \in M_r(\{0,1\})$. *Se puede demostrar que* $\operatorname{tr}((A_r)^n) = L_n^{(r)}$ *para cada* $n \geq 1$. *Así, por el Ejemplo* 2.5, $L^{(r)}$ *es realizable. He aquí la pregunta básica: ¿Es cada sucesión* r*–Fibonacci realizable un múltiplo de* $L^{(r)}$*? Ésta es trivial para* $r = 1$, *y para* $r = 2$ *tenemos el Teorema* 3.4. *Para* $r \geq 3$ *esta pregunta es del interés.*

Para cada $r \in \mathbb{N}$, *definamos la sucesión* r*–Fibonacci,* $F^{(r)}$, *como la sucesión que satisface* (7), *con* $F_r^{(r)} = 1$ *y* $F_n^{(r)} = 0$ *para* $1 \leq n \leq r-1$. *Así,* $F^{(2)}$ *es la sucesión de Fibonacci clásica,* F. *Las propiedades de divisibilidad de* F *han sido estudiadas ampliamente. Por esta razón, en* (4), *se ha expresado cada sucesión* 2*–Fibonacci en términos de* F. *Del mismo modo, para* $r \geq 3$, *podríamos expresar cada sucesión* r*–Fibonacci en términos de* $F^{(r)}$. *Sin embargo, desconocemos estudios similares de* $F^{(r)}$ *para* $r \geq 3$.

4. Temas de Tesis

En esta sección presentamos una serie de posibles temas de tesis relacionados con este trabajo; como el lector se habrá percatado, en el trabajo se han planteado una serie de problemas y preguntas; precisamente desarrollar un trabajo que tenga por objetivo resolver y dar respuesta a estos problemas y preguntas, respectivamente, dando los antecedentes necesarios constituyen los temas de tesis, así se proponen en concreto los siguientes temas:

1. **Caracterizar los polinomios con coeficientes racionales que son realizables.**
2. **Caracterizar las progresiones geométricas de enteros no negativos que son realizables.**
3. **Caracterizar las sucesiones que satisfacen una relación de recurrencia de segundo orden lineal con coeficientes enteros que son realizables.**
4. **Realizar un trabajo sobre positividad de sucesiones.**
5. **Realizar un trabajo sobre divisivilidad de sucesiones.**
6. **Realizar un trabajo, dando los antecedentes, de la demostración de la Proposición 3.7.**
7. **Realizar un trabajo sobre la realización de sucesiones r–Fibonacci, centrado en la pregunta planteada en el Comentario 3.4.**
8. **Realizar un trabajo sobre la representación de sucesiones r–Fibonacci en términos de $F^{(r)}$ para $r \geq 3$.**
9. **Realizar un trabajo sobre funciones aritméticas y realización de sucesiones.**
10. **Realizar un trabajo sobre la estructura algebraica del conjunto de sucesiones realizables.**

La lista podría continuarse, pero consideramos pertinente no extenderla mas. Sin embargo, si algún estudiante tuviera interés en este tema, pero en un contexto de análisis real o complejo, topología, teoría de grupos, de anillos o de campos, podríamos proponer un tema de tesis que se ajuste al interés del alumno y a los requerimientos de la Institución.

Referencias

[1] T.M. Apostol, Introduction to Analytic Number Theory, Springer, New York, 1976.

[2] George Bachman, Introduction to p–Adic Numbers and Valuation Theory, Academic Press, New York and London, 1964.

[3] George L. Cain, Introduction to General Topology, Addison-Wesley, Reading MA, 1994.

[4] V. Chothi, G. Everest and T. Ward, S–integer dynamical systems: periodic points, J. für die Riene Angew. Math. 489 (1997), 99–132.

[5] Toby Hall, The creation of horseshoes, Nonlinearity, 7 (1994), no. 3, 861–924.

[6] G.H. Hardy and E.M. Wright, An Introduction to the Theory of Numbers, fifth ed., Clarendon Press, Oxford, 1979.

[7] D.A. Lind Dynamical properties of quasihyperbolic toral automorphisms, Ergod. Th. Dynam. Sys. 2 (1982), 49–68.

[8] D. Lind and B. Marcus, Symbolic Dynamics and Coding, Cambridge University Press, Cambridge, 1995.

[9] E. Lucas, Théorie des functions numériques simplement périodiques, Amer. J. Math. 1 (1878), 184–240, 289–321.

[10] W.K. Nicholson, Introduction to Abstract Algebra, John Wiley & Sons, New York, 1999.

[11] P. Ribenboim, The Fibonacci numbers and the Arctic Ocean. In M. Behara, R. Fritsch, and R. G. Lintz, editors, Symposia Gaussian, Conf. A (Proceedings of the Second Gaussian Symposium, München), pages 41–83, W. de Gruyter, Berlin, 1995.

[12] A.N. Sharkovskiĭ, Coexistence of cycles of a continuous map of the line into itself, Ukrain Mat. Zh. 16 (1964), no. 1, 61–71; Translated by J. Tolosa in Internat. J. Bifurc. Chaos Appl. Sci. Engrg, 5 (1995), no. 5, 1263–1273.

[13] M. Ward, Memoir on elliptic divisibility sequences, Amer. J. Math. 70 (1948), 31–74.

Fracciones continuas: cuatro aplicaciones

Mario Pineda Ruelas
Universidad Autónoma Metropolitana–I
División de Ciencias Básicas e Ingeniería,
Departamento de Matemáticas,
C.P. 09340 México D.F., México.
mpr@xanum.uam.mx

Resumen

En estas notas daremos un paseo por la teoría clásica de las fracciones continuas a partir de hechos elementales, así como su aplicación a la solución de algunos problemas en teoría de números. Muchas teorías matemáticas no surgen de la nada, surgen precisamente de la experimentación y la observación: sí, la matemática también es una ciencia experimental. Estos serán los componentes principales de nuestro desarrollo: la experimentación y la observación.

1. Introducción

Escribiendo un trabajo de matemáticas, el profesor Ezra Brown [1] teclea accidentalmente $g - 1$ en lugar de g^{-1}. Uno de sus estudiantes descubre el error y le hace notar que el error no tiene importancia. Una hipótesis adicional era $g > 0$. Si resolvemos la igualdad $g - 1 = g^{-1}$ descubrimos rápidamente que g debe ser una raíz del polinomio $g^2 - g - 1 = 0$ y por lo tanto $g = \dfrac{1+\sqrt{5}}{2}$, la razón dorada que tanto inspiró a los griegos. Si observamos la igualdad $g = 1 + \dfrac{1}{g}$ y olvidamos por un momento el valor de

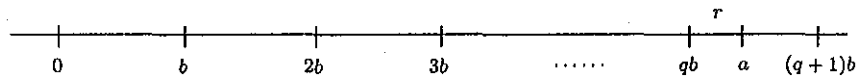
[0]Palabras clave: Fracciones continuas, AMS Clasification 11A55.

g, podemos preguntarnos si la expresión

$$g = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}}}}$$

es un número (¿convergencia?). Sirva este accidente como introducción al tema que queremos desarrollar.

Una versión elemental de aproximación entre dos enteros lo brinda el célebre algoritmo de la división: si a, b son enteros y $b \neq 0$, existen únicos q, r tal que $a = qb + r$ con $0 \leq r < |b|$. Para imaginar el por qué es una versión elemental de aproximación supongamos que $a, b > 0$. Observemos la siguiente gráfica:



Sin duda alguna, el modelo de elegancia en toda la matemática es el *algoritmo euclidiano de la división* en el anillo de los enteros $\mathbb{Z}$. Esto se debe a la simplicidad de su planteamiento y ejecución no sólo en computadoras. Cualquier libro elemental de álgebra o teoría de números incluye una prueba y casi cualquiera de ellas describe explícitamente cómo encontrar el *máximo común divisor* entre dos enteros.

Teorema 1.1. [Algoritmo de Euclides] *Sean a, b enteros diferentes de 0. Entonces, después de aplicar el algoritmo de la división varias veces obtenemos*

$$\begin{aligned}
a &= bq_1 + r_1 && 0 < r_1 < |b|,\\
b &= r_1q_2 + r_2 && 0 < r_2 < r_1,\\
r_1 &= r_2q_3 + r_3 && 0 < r_3 < r_2,\\
&\vdots \quad \vdots\\
r_{k-2} &= r_{k-1}q_k + r_k && 0 < r_k < r_{k-1},\\
r_{k-1} &= r_kq_{k+1},
\end{aligned}$$

y donde $r_k = \mathrm{mcd}(a, b)$.

Ejemplo 1.2. *Calculemos* mcd(32, 245):

$$245 = 32 \cdot 7 + 21, \tag{1}$$
$$32 = 21 \cdot 1 + 11, \tag{2}$$
$$21 = 11 \cdot 1 + 10, \tag{3}$$
$$11 = 10 \cdot 1 + 1, \tag{4}$$
$$10 = 1 \cdot 10 + 0. \tag{5}$$

Así que mcd(32, 245) = 1.

2. Fracciones continuas

Antes de dar la definición formal de lo que es una fracción continua, desarrollaremos una expresión para el racional $\frac{245}{32}$. De (1) tenemos:

$$\frac{245}{32} = 7 + \frac{21}{32} \tag{6}$$

De (2) observamos que $\frac{32}{21} = 1 + \frac{11}{21}$. Por lo tanto $\frac{21}{32} = \frac{1}{1 + \frac{11}{21}}$.

Sustituimos ahora en (6) para obtener:

$$\frac{245}{32} = 7 + \frac{1}{1 + \frac{11}{21}} \tag{7}$$

De (3) tenemos $\frac{21}{11} = 1 + \frac{10}{11}$ y así $\frac{11}{21} = \frac{1}{1 + \frac{10}{11}}$.

Sustituyendo en (7) tenemos:

$$\frac{245}{32} = 7 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{10}{11}}} \tag{8}$$

Ahora, para $\frac{10}{11}$, observamos en (4) que $\frac{11}{10} = 1 + \frac{1}{10}$ y sustituyendo en (8)

el inverso multiplicativo de $\frac{11}{10}$

$$\frac{245}{32} = 7 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{10}}}} \tag{9}$$

Podemos usar la notación $\frac{245}{32} = [7; 1, 1, 1, 10]$ donde la sucesión $7, 1, 1, 1, 10$ es fácilmente identificable desde (6) hasta (9). Notemos la representación decimal $\frac{245}{32} = 7.\overline{65625}$ y por el momento no observamos alguna relación entre las expresiones $[7; 1, 1, 1, 10]$ y $7.\overline{65625}$.

Definición 2.1. *Una fracción continua simple es una expresión de la forma*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}}$$

donde los $a_i \in \mathbb{N}$ *para* $i \geq 1$ *y* $a_0 \in \mathbb{Z}$. *Escribiremos* $[a_0; a_1, a_2, ...]$ *para indicar a la fracción continua.*

Notamos que en nuestro ejemplo, los números $7, 1, 1, 1, 10$ son justamente los cocientes q_i que aparecen en el algoritmo de Euclides.

Teorema 2.2. *Sea* $\frac{a}{b} \in \mathbb{Q}$ *con* $b > 0$. *Entonces* $\frac{a}{b} = [q_1; q_2, ..., q_k, q_{k+1}]$, *donde los* q_i *se obtienen al calcular* $\text{mcd}(a, b)$ *a partir del algoritmo de Euclides.*

La demostración consiste simplemente en calcular el $\text{mcd}(a, b)$ con el algoritmo de Euclides y despejar tal como lo hicimos en el ejemplo. Así que en pocas palabras, el teorema anterior nos asegura que cualquier número racional se puede expresar como una fracción continua simple con un número finito de entradas. ¿Es única la representación? La respuesta es no. La última entrada en $[q_1; q_2, ..., q_k, q_{k+1}]$ o es 1 o es $\neq 1$. Así:

Si $q_{k+1} = 1$, entonces

$$[q_1; q_2, ..., q_k, 1] = [q_1; q_2, ..., q_{k-1}, q_{k+1}]$$

y si $q_{k+1} > 1$,

$$[q_1; q_2, \cdots, q_{k+1}] = [q_1; q_2, \cdots, q_k, q_{k+1} - 1, 1].$$

Así, podemos jugar con la paridad de la longitud de las fracciones continuas finitas. En nuestro ejemplo tenemos:

$$[7; 1, 1, 1, 10] = [7; 1, 1, 1, 9, 1].$$

¿Cualquier número real se puede representar como una fracción continua? La respuesta es sí. En lo que sigue $[x]$ indicará el mayor entero menor o igual a x. Veamos algunos ejemplos de fracción continua simple de números irracionales.

Ejemplo 2.3. *Sea $x = \pi$ con la aproximación decimal $\pi \sim 3.14159265359$.*

Sea $a_0 = [\pi] = 3$. Por lo tanto $\pi = 3 + .14159265359$.

Manipulando $.14159265359 = \dfrac{14159265359}{10^{11}}$ *obtenemos*

$$\begin{aligned} \pi &= 3 + .14159265359 = 3 + \cfrac{1}{\cfrac{10^{11}}{14159265359}} \\ &= 3 + \cfrac{1}{7 + .062513305921}, \end{aligned}$$

donde $a_1 = \left[\dfrac{10^{11}}{14159265359}\right] = 7$. *Ahora estudiemos* $.062513305921$.

Puesto que $.062513305921 = \dfrac{62513305921}{10^{12}}$, *tenemos*

$$.062513305921 = \cfrac{1}{\cfrac{10^{12}}{62513305921}} = \cfrac{1}{15 + .996594409256},$$

donde $a_2 = \left[\dfrac{10^{12}}{62513305921}\right] = 15$. *Por lo tanto:*

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + .996594409256}}.$$

Continuando con el algoritmo:

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \ddots}}}}}}}}}}$$

y así podemos escribir:

$$\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, 2, 2, 2, 1, 84, 2, 1, ...].$$

Ejemplo 2.4. *Sea* $x = \dfrac{1+\sqrt{11}}{3}$ *con la aproximación* 1.438874930118466. *Es claro que* $a_0 = [x] = 1$ *y* $x = 1 + .438874930118466$. *Manipulando la parte decimal tenemos:*

$$.438874930118466 = \frac{438874930118466}{10^{15}} = \frac{1}{\dfrac{10^{15}}{438874930118466}}$$

$$= \frac{1}{2 + .278553481580889}.$$

Así $x = 1 + \dfrac{1}{2 + .278553481580889}$. *Repitiendo el mismo argumento:*

$$.278553481580889 = \frac{278553481580889}{10^{15}} = \frac{1}{\dfrac{10^{15}}{278553481580889}}$$

$$= \frac{1}{3 + .5899748742131967}.$$

Así que podemos escribir:

$$x = 1 + \cfrac{1}{2 + \cfrac{1}{3 + .5899748742131967}}.$$

Después de repetir el algoritmo varias veces, llegamos a

$$\frac{1+\sqrt{11}}{3} = [1; 2, 3, 1, 1, 2, 3, 1, 1, 2, 3, 1, 1, 2, 3, 1, ...].$$

El siguiente resultado describe formalmente la manera de encontrar el desarrollo de la fracción continua que representa a un número real.

Teorema 2.5. [Algoritmo de las fracciones continuas] *Si $x \notin \mathbb{Q}$, entonces x se puede representar como una fracción continua infinita simple.*

Demostración: Sea $a_0 = [x]$. Puesto que $x \neq [x]$, entonces existe $r_1 \in \mathbb{R}$ positivo tal que $x = a_0 + \frac{1}{r_1}$. Notemos que $0 < \frac{1}{r_1} < 1$. Sea $a_1 = [r_1]$. Claramente $a_1 \neq r_1$ pues de lo contrario $x \in \mathbb{Q}$. Así tenemos que $r_1 = a_1 + \frac{1}{r_2}$ para cierto $r_2 \in \mathbb{R}$ positivo y $0 < \frac{1}{r_2} < 1$. En este momento lo que hemos logrado es lo siguiente:

$$x = a_0 + \frac{1}{r_1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{r_2}}.$$

Notemos que si continuamos este proceso, en ningún momento obtendremos que $a_i = r_i$, ya que de lo contrario x sería racional. Sólo nos falta mostrar que este proceso infinito produce una fracción continua simple que converge a x. Antes necesitamos más conceptos.

□

Sea $[a_0; a_1, a_2, ..., a_n, ...]$ y la fracción parcial $[a_0, a_1, a_2, ..., a_n]$. Puesto que las entradas son enteros, entonces observamos que:

$$[a_0, a_1, a_2, ..., a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}$$

es un número racional. Denotamos $[a_0, a_1, a_2, ..., a_n] = \frac{p_n}{q_n}$ y lo llamaremos el n-ésimo convergente de $[a_0; a_1, a_2, ..., a_n, ...]$. Observemos las siguientes fracciones continuas finitas:

$$[a_0] = \frac{a_0}{1}, \quad [a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_1 a_0 + 1}{a_1}, \quad [a_0; a_1, a_2] = \frac{a_2 a_1 a_0 + a_2 + a_0}{a_2 a_1 + 1}.$$

Notamos que si $n = 0$, entonces $p_0 = a_0$ y $q_0 = 1$. Si $n = 1$, entonces $p_1 = a_1 a_0 + 1$ y $q_1 = a_1$. Si $n = 2$, entonces $p_2 = a_2 a_1 a_0 + a_2 + a_0$ y $q_2 = a_2 a_1 + 1$.

En general, los convergentes obedecen las siguientes leyes recursivas:

Teorema 2.6. *Sea $[a_0; a_1, ..., a_n]$ el n-ésimo convergente de la fracción continua $[a_0; a_1, ..., a_n, ...]$. Si $n \geq 2$, entonces $[a_0; a_1, ..., a_n] = \frac{p_n}{q_n}$ donde*

$$p_n = a_n p_{n-1} + p_{n-2} \quad y \quad q_n = a_n q_{n-1} + q_{n-2}.$$

Demostración: Inducción sobre n. La observación previa al enunciado de nuestro teorema es precisamente el caso $n = 2$. Supongamos cierta la afirmación para n. Es fácil verificar que

$$[a_0; a_1, ..., a_n, a_{n+1}] = [a_0; a_1, ..., a_{n-1}, a_n + \frac{1}{a_{n+1}}].$$

Así tenemos:

$$\left[a_0; a_1, ..., a_{n-1}, a_n + \frac{1}{a_{n+1}}\right] = \frac{\left(a_n + \frac{1}{a_{n+1}}\right) p_{n-1} + p_{n-2}}{\left(a_n + \frac{1}{a_{n+1}}\right) q_{n-1} + q_{n-2}}$$

$$= \frac{a_{n+1}\left[\left(a_n + \frac{1}{a_{n+1}}\right) p_{n-1} + p_{n-2}\right]}{a_{n+1}\left[\left(a_n + \frac{1}{a_{n+1}}\right) q_{n-1} + q_{n-2}\right]} = \frac{a_{n+1}(a_n p_{n-1} + p_{n-2}) + p_{n-1}}{a_{n+1}(a_n q_{n-1} + q_{n-2}) + q_{n-1}}$$

$$= \frac{a_{n+1} p_n + p_{n-1}}{a_{n+1} q_n + q_{n-1}} = \frac{p_{n+1}}{q_{n+1}}.$$

□

Si definimos $p_{-1} = 1,\ p_{-2} = 0,\ q_{-1} = 0,\ q_{-2} = 1$, entonces las fórmulas también son válidas para $n = 0, 1$.

Repasando la prueba del Teorema 2.6 podemos preguntarnos ¿en dónde usamos que los a_i's son enteros positivos? Obviamente en ninguna parte. Así, las leyes recursivas son válidas si las entradas a_i son números reales positivos para $i \geq 1$.

Regresamos a nuestros ejemplos. Si escribimos $x_n = \dfrac{p_n}{q_n}$, entonces para la fracción continua de $x = \dfrac{1+\sqrt{11}}{3} = 1.438874930118466$ tenemos:

n	a_n	p_n	q_n	x_n	
0	1	1	1	1	$x_0 < x$
1	2	3	2	1.5	$x_1 > x$
2	3	10	7	1.42857142857142	$x_2 < x$
3	1	13	9	1.444444444	$x_3 > x$
4	1	23	16	1.4375	$x_4 < x$
5	2	59	41	1.439024390243	$x_5 > x$
6	3	200	139	1.438848920863	$x_6 < x$
7	1	259	180	1.438888888888	$x_7 > x$
8	1	459	319	1.438871473354	$x_8 < x$
9	2	1177	818	1.438875305623	$x_9 > x$
10	3	3990	2773	1.438874864760	$x_{10} < x$

y para $x = \pi$:

n	a_n	p_n	q_n	x_n	
0	3	3	1	3	$x_0 < \pi$
1	7	22	7	3.142857142857	$x_1 > \pi$
2	15	333	106	3.141509433962	$x_2 < \pi$
3	1	355	113	3.141592920354	$x_3 > \pi$
4	292	103993	33102	3.141592653012	$x_4 < \pi$
5	1	104348	33215	3.141592653921	$x_5 > \pi$
6	1	208341	66317	3.141592653467	$x_6 < \pi$
7	1	312689	99532	3.141592653619	$x_7 > \pi$
8	2	833719	265381	3.141592653581	$x_8 < \pi$
9	1	1146408	364913	3.141592653591	$x_9 > \pi$
10	3	5419351	1725033	3.14159265358	$x_{10} < \pi$

En cualquiera de los dos casos observamos que los convergentes generan dos sucesiones monótonas: una creciente, otra decreciente y ambas acotadas por x. ¡Que convergencia tan espectacular! En general tenemos:

Teorema 2.7. *Los convergentes de* $[a_0, a_1, a_2, ..., a_n, ...]$ *satisfacen:*

$$x_0 < x_2 < ... < x_{2n} < \cdots < x < \cdots < x_{2n-1} < \cdots < x_3 < x_1,$$

y por lo tanto $\lim_{n\to\infty} x_{2n} = \lim_{n\to\infty} x_{2n+1} = x$.

□

Este comportamiento de los convergentes garantiza la convergencia en el Teorema 2.5. En los tres ejemplos que hemos estudiados notamos diferencias:

1. En el Ejemplo 1.2 la longitud de la fracción continua es finita.
2. Los Ejemplos 2.3 y 2.4 tienen una infinidad de entradas.
3. En el Ejemplo 2.4, se repite el bloque $1, 2, 3, 1$.

El Ejemplo 2.4 es de nuestro interés. Podemos escribir:

$$\frac{1+\sqrt{11}}{3} = [1; 2, 3, 1, 1, 2, 3, 1, 1, 2, 3, 1, 1, 2, 3, 1, ...] = [\overline{1; 2, 3, 1}],$$

tal como se hace al escribir la representación decimal de un número real periódico. De esta forma, resulta natural decir que $[\overline{1; 2, 3, 1}]$ es una fracción continua periódica de longitud 4. Otros ejemplos de fracciones continuas periódicas:

1. $[2; 3, 7, 2, \overline{3, 5, 4, 9, 5, 5, 7}]$ tiene período 7.
2. $[3; \overline{2, 2, 6}]$ tiene período 3.
3. $[1; 1, 1, 1, 1, , , ,] = \dfrac{1+\sqrt{5}}{2}$ tiene período 1.

Formalmente la periodicidad la podemos definir como:

Definición 2.8. *Diremos que* $[a_0; a_1, ..., a_n, a_{n+1}, ...]$ *es una fracción continua periódica si existe* $k \geq 0$ *y* $s \in \mathbb{N}$ *tal que* $a_i = a_{s+i}$ *para* $i > k$. *Al menor entero* s *que satisface la condición anterior lo llamaremos período de la fracción y al arreglo ordenado* $a_0, a_1, ..., a_k$ *lo llamaremos preperíodo.*

La definición de fracción continua periódica es más clara si escribimos:

$$[a_0; a_1, ..., a_k, a_{k+1}, ..., a_{k+s}, a_{k+1}, ..., a_{k+s}, ...],$$

y en este caso la notación más apropiada es:

$$[a_0; a_1, ..., a_k, \overline{a_{k+1}, ..., a_{k+s}}].$$

En particular, si $x = [\overline{a_0; a_1, a_2, ..., a_n}]$, entonces podemos escribir $x = [a_0; a_1, a_2, ..., a_n, x]$. Aplicando el Teorema 2.6 tenemos:

$$x = \frac{xp_n + p_{n-1}}{xq_n + q_{n-1}},$$

y por lo tanto $x^2q_n + x(q_{n-1} - p_n) - p_{n-1} = 0$. Así, un número irracional cuya fracción continua es periódica es raíz de algún polinomio con coeficientes en $\mathbb{Z}$. Inversamente, si un número irracional es raíz de algún polinomio cuadrático no trivial en $\mathbb{Z}[x]$, entonces la fracción continua de x es periódica. Esta clase de números se llaman *irracionales cuadráticos.*

Teorema 2.9. *Sea x un irracional cuadrático. Entonces la fracción continua que representa a x es periódica.*

Demostración: [2] Theorem 177.

Ahora sabemos que la fracción continua de π no puede ser periódica pues de lo contrario, π sería algebraico.

Un caso particularmente importante, y de ahí nuestro interés, es la fracción continua de $\sqrt{d}$ donde d es un entero positivo que no es un cuadrado. Se puede mostrar con un poco de cuidado que:

$$\sqrt{d} = [a_0; \overline{a_1, ..., a_{n-1}, 2a_0}],$$

donde $a_i = a_{n-i}$ para $i = 1, 2, ..., n-1$ y $a_0 = [\sqrt{d}]$. Por ejemplo

$$\sqrt{2047} = [45; \overline{4, 9, 1, 4, 8, 45, 8, 4, 1, 9, 4, 90}].$$

3. Aplicaciones

3.1. Ecuación de Pell

Sea d es un entero positivo que no es un cuadrado. Consideremos la extensión cuadrática $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$. Asociado al campo $\mathbb{Q}(\sqrt{d})$ se encuentra el

anillo *de enteros cuadráticos*:

$$\mathcal{O}_d = \{\alpha \in \mathbb{C} : \alpha \text{ es raíz de algún polinomio mónico en } \mathbb{Z}[x]\} \cap \mathbb{Q}(\sqrt{d}).$$

Se puede dar la descripción explícita del anillo $\mathcal{O}_d$ ([3] Proposition 13.1.1):

1. Si $d \equiv 2, 3 \pmod 4$, entonces $\mathcal{O}_d = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$.

2. Si $d \equiv 1 \pmod 4$, entonces $\mathcal{O}_d = \{a + b\left(\frac{-1+\sqrt{d}}{2}\right) : a, b \in \mathbb{Z}\}$.

Justamente la diferencia entre el anillo $\mathcal{O}_d$ y el campo $\mathbb{Q}(\sqrt{d})$ es que no todos los elementos de $\mathcal{O}_d$ tienen inverso multiplicativo (unidades). Con ayuda de la función norma en el caso $d \equiv 2, 3 \pmod 4$ se puede encontrar el grupo multiplicativo de los elementos invertibles en el anillo $\mathcal{O}_d$. Así tenemos que si $a + b\sqrt{d} \in \mathcal{O}_d$, entonces la norma es definida como $\mathbf{N}(a + b\sqrt{d}) = a^2 - db^2$ y $a + b\sqrt{d}$ tiene inverso multiplicativo en $\mathcal{O}_d$ si y sólo si $\mathbf{N}(a + b\sqrt{d}) = a^2 - db^2 = \pm 1$. Teóricamente, la manera más eficiente, de resolver la ecuación $a^2 - db^2 = \pm 1$ es usando los convergentes de la fracción continua de $\sqrt{d}$. Veamos un ejemplo:

Ejemplo 3.1. *Encontraremos algunas unidades en el anillo $\mathcal{O}_7$ resolviendo $x^2 - 7y^2 = \pm 1$.*

n	a_n	p_n	q_n	$p_n^2 - 7q_n^2 =$
0	2	2	1	-3
1	1	3	1	2
2	1	5	2	-3
3	1	8	3	1
4	4	37	14	-3
5	1	45	17	2
6	1	82	31	-3
7	1	127	48	1
8	4	590	223	-3
9	1	717	271	2
10	1	1307	494	-3
11	1	2024	765	1

Observemos la igualdad $p_n^2 - 7q_n^2 = (p_n - q_n\sqrt{7})(p_n + q_n\sqrt{7})$. Así por ejemplo, ubicándonos en el cuarto renglón poniendo $x = 8$, $y = 3$ tenemos

$$8^2 - 7 \cdot 3^2 = (8 - 3\sqrt{7})(8 + 3\sqrt{7}) = 1.$$

Por lo tanto, $8-3\sqrt{7}$ y $8+3\sqrt{7}$ son elementos de $\mathcal{O}_7$ y son unidades. Fijemos nuestra atención en el número $8+3\sqrt{7}$:

$$(8+3\sqrt{7})^2 = 127+48\sqrt{7},$$
$$(8+3\sqrt{7})^3 = 2024+765\sqrt{7},$$
$$(8+3\sqrt{7})^4 = 32257+12192\sqrt{7}.$$

Al menos observamos que la solución localizada en el cuarto renglón, elevándola a potencias genera otras soluciones. Esto efectivamente es así:

Teorema 3.2. *Supongamos $d > 0$ tal que d no es un cuadrádo. Entonces:*

1. *La ecuación $x^2 - dy^2 = 1$ siempre es soluble en $\mathbb{N}$.*
2. *Si $a^2 - db^2 = 1$ y $a, b \in \mathbb{N}$, entonces $\frac{a}{b}$ es algún convergente de la fracción continua de $\sqrt{d}$.*
3. *Existen $a, b > 0$ mínimos tal que cualquier solución de $x^2 - dy^2 = 1$ se puede escribir como $(a+b\sqrt{d})^n$ y $n \in \mathbb{Z}$.*
4. *El conjunto de soluciones de la ecuación de Pell $x^2 - dy^2 = 1$ descritas en el punto anterior es un grupo cíclico isomorfo a $\mathbb{Z}$.*
5. *El conjunto de todas las soluciones de $x^2 - dy^2 = 1$ está descrito por el grupo $\{\pm(a+b\sqrt{d})^n : n \in \mathbb{Z}\} \simeq \{1,-1\} \times \mathbb{Z}$, donde a, b son como en el punto 3.*

Notemos la importancia de la parte 2: ésta nos indica en dónde buscar las soluciones positivas. La parte 3 nos dice que si encontramos la *menor* solución, habremos resuelto el problema de conocer los elementos invertibles del anillo $\mathcal{O}_d$. Teóricamente es posible resolver la ecuación de Pell, pero computacionalmente existen muchos problemas porque calcular los convergentes puede producir números enteros muy grandes.

Algunas preguntas que quedan pendientes:

1. ¿Existen anillos que tienen unidades con norma -1?
2. ¿Tiene alguna relación la longitud del período con la pregunta anterior?
3. ¿Qué otros problemas se pueden atacar ya conociendo las unidades de un anillo cuadrático?

4. ¿Si $d < 0$ cómo son las unidades?

5. ¿Existen ecuaciones similares a la de Pell que la generalizan?

La respuesta a las preguntas 1 y 2 es: Sea l la longitud del período de $\sqrt{d}$. Si l es par, entonces las soluciones positivas de $x^2 - dy^2 = 1$ caen precisamente en las entradas $ls-1$ y la ecuación $x^2-dy^2 = -1$ no es soluble. Si l es impar, las soluciones positivas a $x^2 - dy^2 = -1$ se localizan en las entradas $2sl - 1$ y las soluciones positivas de $x^2 - dy^2 = 1$ están ubicadas en las entradas $2(s-1)l - 1$, es decir, si l es impar, entonces existen unidades con norma 1 y -1 [6]. Con respecto a la pregunta 3, conociendo las unidades se pueden resolver cierta clase de ecuaciones polinomiales con coeficientes en $\mathbb{Z}$ (ver por ejemplo Theorem 4.20 en [8]) y la táctica es estudiar la ecuación en algún anillo cuadrático, buscar las soluciones y luego regresar. Esta fue la filosofía que se utilizó para resolver *La Conjetura de Fermat.* Para la pregunta 4 la respuesta se encuentra en el siguiente resultado:

Teorema 3.3. *Sea $d < 0$ un entero libre de cuadrados. Entonces:*

1. *Si $d = -1$, entonces las unidades de $\mathcal{O}_{-1}$ son $\{\pm 1, \pm i\}$.*

2. *Si $d = -3$, entonces las unidades de $\mathcal{O}_{-3}$ son $\{\pm 1, \pm\rho, \pm\rho^2\}$, donde $\rho^3 = 1$ y $\rho \neq 1$.*

3. *Si $d = -2$ o $d < -3$, entonces las unidades de $\mathcal{O}_d$ son $\{\pm 1\}$.*

Demostración: Consultar [3] Proposition 13.1.5.

□

En respuesta a la pregunta 5 invitamos al lector para que consulte [5].

3.2. Factorización de enteros

Método de Shanks. Supongamos que queremos factorizar el entero $d > 1$ el cual sospechamos que no es un cuadrado, por ejemplo estudiando su residuo al ser dividido entre 4. El problema es sencillo de plantear: factorizar d. Bueno, lo primero que intentamos es encontrar enteros x, y tal que $x^2 - dy^2 = r^2$. Para esto utilizamos una propiedad que satisfacen los convergentes:

$$p_{i-1}^2 - dq_{i-1}^2 = (-1)^i k_i,$$

donde k_i es algún entero positivo (Theorem 5.3.4 en [4]). Por supuesto que debemos buscar cuándo el respectivo k_i es un cuadrado perfecto para algún i par. Suponiendo que lo logramos. Entonces el paso siguiente es observar que

en la factorización $dq_{i-1}^2 = p_{i-1}^2 - k_i = (p_{i-1} - \sqrt{k_i})(p_{i-1} + \sqrt{k_i})$ se tiene que algunos de los factores primos de $p_{i-1} - \sqrt{k_i}$ y $p_{i-1} + \sqrt{k_i}$ son factores de d. Claro está que este método involucra el período de $\sqrt{d}$. El siguiente paso es usar el algoritmo de Euclides para encontrar los números $\text{mcd}(d, p_{i-1} - \sqrt{k_i})$ y $\text{mcd}(d, p_{i-1} + \sqrt{k_i})$. El método puede fracasar en algunos casos:

1. El período de la fracción continua de $\sqrt{d}$ es muy corto.
2. Los valores de p_i y q_i tienden a ser muy grandes.
3. $d \mid p_i + \sqrt{k_i}$ y $\text{mcd}(d, p_i - \sqrt{k_i}r) = 1$ o viceversa.

Por ejemplo, el método no funciona con $d = 1313$ pues $\sqrt{1313} = [36; \overline{4, 4, 72}]$ y $k_{2n} = 17$, aún cuando $1313 = 13 \cdot 101$. Veamos un ejemplo en donde si funciona el método de Shanks. Sea $d = 29041$. Se puede verificar que:

$$\sqrt{29041} = [170; \overline{2, 2, 2, 2, 2, 340}].$$

Puesto que $a_0 = 170, a_1 = 2, a_2 = 2, a_3 = 2, a_4 = 2, a_5 = 2, a_6 = 340$, por el Teorema 2.6 tenemos que para $i = 4$:

$$p_3 = 2045, \quad q_3 = 12,$$

y por lo tanto

$$p_3^2 - dq_3^2 = 4182025 - 4181904 = 11^2.$$

Así que $(2045)^2 - 11^2 = (2045 + 11)(2045 - 11) = 29041 \cdot 12^2$ y puesto que $\text{mcd}(29041, 2045 - 11) = 113$ y $\text{mcd}(29041, 2045 + 11) = 257$, hemos encontrado un par de factores del número 29041. Coincidentemente $29041 = 113 \cdot 257$.

Finalmente, por fortuna no hay métodos cien por ciento efectivos, unos mejores que otros. Esta dificultad ha despertado el interés de grupos de investigadores en todo el mundo, especialmente en teoría de números y computación. Invitamos al lector para que revise [9], el cual es un referente en el tema.

3.3. Clasificación de números enteros

¿Cuáles son los números reales cuya representación como fracción continua tiene período 1? Observemos lo siguiente: Si x es tal número, entonces

$x = [a; \overline{2a}]$. Así

$$x = a + \cfrac{1}{2a + \cfrac{1}{2a + \cfrac{1}{\ddots}}}$$

Por lo tanto

$$x - a = \cfrac{1}{2a + \cfrac{1}{2a + \cfrac{1}{\ddots}}}$$

y así tenemos $x = a + \dfrac{1}{2a + x - a} = a + \dfrac{1}{x + a}$. Resolviendo llegamos a que $x = \sqrt{a^2 + 1}$. ¿De qué forma son los números reales cuya representación en fracción continua es periódica de período 2? ¿y de periódo k? Al respecto invitamos al lector para que consulte [7].

3.4. Encriptando con el grupo simétrico S_n

Nuestra lengua española consta de un alfabeto de 27 letras sin contar *ch* y *ll*. Llamemos $\mathcal{A}$ al conjunto de letras del alfabeto y $I_{27} = \{1, 2, 3, ..., 27\}$. Consideremos cualquier función biyectiva $f : \mathcal{A} \to I_{27}$. Entonces cualquier palabra se puede considerar como un arreglo de la forma:

$$f(a_1)f(a_2)\cdots f(a_r),$$

donde $a_j \in \mathcal{A}$ y $f(a_j)$ es la imagen de una de las letras que componen a la palabra. Así por ejemplo, si f es la función:

a→1	e→5	i→9	m→13	p→17	t→21	x→25
b→2	f→6	j→10	n→14	q→18	u→22	y→26
c→3	g→7	k→11	ñ→15	r→19	v→23	z→27
d→4	h→8	l→12	o→16	s→20	w→24	

entonces la frase *que padre está esto* se puede escribir como

18 22 5 17 1 4 19 5 5 20 21 1 5 20 21 16.

Por supuesto que no asignamos algún indicador especial para los acentos pues se trata de esconder mensajes y entre menos pistas, más complicado para el que intenta leer.

Ahora, si pensamos que cada arreglo de números es la fracción continua de un número racional tendremos que:

$$18\ 22\ 5 = [18; 22, 5] = \frac{2003}{111},$$

$$17\ 1\ 4\ 19\ 5 = [17; 1, 4, 19, 5] = \frac{8634}{485},$$

$$5\ 20\ 21\ 1 = [5; 20, 21, 1] = \frac{2227}{441},$$

$$5\ 20\ 21\ 16 = [5; 20, 21, 16] = \frac{34117}{6756}.$$

Por lo tanto, la frase *que padre está esto* escrito con números racionales queda como:

$$\frac{2003}{111}\ \frac{8634}{485}\ \frac{2227}{441}\ \frac{34117}{6756}.$$

Notemos que:

1. Si queremos recuperar el mensaje conociendo de antemano los números racionales y la función biyectiva f, entonces sólo se tiene que escribir la fracción continua de cada uno de los números y luego aplicar la imagen inversa de cada una de las entradas.

2. Si damos el orden natural a las letras del alfabeto tal como estamos acostumbrados, entonces podemos pensar, en nuestro ejemplo, que f es la función identidad.

3. Es una ventaja tremenda conocer la información de los dos puntos anteriores.

Ahora supongamos que queremos leer el mensaje:

$$\frac{119336503}{40360652}\ \frac{17147}{1214}\ \frac{1212301}{120786},$$

y es la única información que tenemos a la mano. Bueno, lo primero que se debe hacer es dar la fracción continua de cada número racional que aparece

en el mensaje:

$$\begin{aligned}\frac{119336503}{40360652} &= [2;1,22,8,9,8,22,22,6],\\ \frac{17147}{1214} &= [14;8,25,6],\\ \frac{1212301}{120786} &= [10;27,5,19,9,5].\end{aligned}$$

Así, nuestro mensaje queda escrito como:

$$[2;1,22,8,9,8,22,22,6]\quad[14;8,25,6]\quad[10;27,5,19,9,5],$$

o sin los corchetes:

$$2\ 1\ 22\ 8\ 9\ 8\ 22\ 22\ 6\quad 14\ 8\ 25\ 6\quad 10\ 27\ 5\ 19\ 9\ 5$$

Qué problemón, pues f es algún elemento del grupo simétrico S_{27} cuyo orden es:

$$27! = 10,888,869,450,418,352,160,768,000,000.$$

Posiblemente en un mensaje corto puede ser complicado hacer un estudio sobre la frecuencia de la presencia de los números en el mensaje, que a final de cuentas puede indicar de qué letra se trata. Otro problema que puede identificarse es que, la frecuencia cambia dependiendo del estilo de la escritura. Así por ejemplo, si el estilo es narrativo, aumenta la frecuencia de la letra r. De cualquier forma, un buen criptoanalista siempre aprovecha las regularidades de un idioma, que es a final de cuentas lo que buscan los científicos en su quehacer diario. A continuación presentamos dos tablas que presentan las frecuencias de cada letra, según el tipo de textos analizados:

a→11.9	e→14.6	i→7.1	m→2.8	p→3.1	t→4.6	x→.2
b→1.1	f→.7	j→.6	n→7.2	q→.5	u→3.3	y→1.1
c→4.8	g→1.3	k→0	ñ→.1	r→6.6	v→.9	z→.4
d→5	h→.3	l→5.5	o→9.1	s→7.2	w→0	

a→12.7	e→13.2	i→11.3	m→2.7	p→2.4	t→3.9	x→.1
b→1.4	f→.5	j→0	n→7	q→1.2	u→4.6	y→1.1
c→3.9	g→1.2	k→0	ñ→0	r→6.3	v→1.1	z→.4
d→5.6	h→1.2	l→5.9	o→9.5	s→7.6	w→0	

En las dos tablas de frecuencias observamos que las vocales suman casi el 46 % del total, en donde las letras a, e se llevan los aplausos. Mientras que las letras c,d,l,n,r,s se llevan el 36.3 % del total. Esta regularidad puede ayudar en determinado momento a decidir de qué letra se trata, aún en mensajes cortos. Los datos de las tablas fueron obtenidos del sitio:

`http://www.cripto.es/enigma/boletin_enigma_32.htm`

Para que el lector se divierta, use la permutación

$1\to5$	$5\to1$	$9\to8$	$13\to19$	$17\to9$	$21\to10$	$25\to20$
$2\to11$	$6\to2$	$10\to4$	$14\to26$	$18\to23$	$22\to16$	$26\to24$
$3\to3$	$7\to21$	$11\to13$	$15\to15$	$19\to27$	$23\to17$	$27\to25$
$4\to7$	$8\to14$	$12\to22$	$16\to6$	$20\to12$	$24\to18$	

y el orden natural del alfabeto, es decir: $a \to 1, b \to 2, c \to 3\ldots$ para descifrar el siguiente mensaje:

$$\frac{119336503}{40360652} \quad \frac{17147}{1214} \quad \frac{1212301}{120786}$$

Agradezco a las autoridades de la Facultad de Matemáticas de la Universidad Veracruzana, Xalapa de Eqz., en especial a los Drs. José Rigoberto Gabriel Argüelles, Raquiel Rufino López Martínez y Arturo Cueto Hernández por su hospitalidad durante el Segundo Taller de Teoría de Números llevado a cabo en el mes de abril del 2007 en las instalaciones de la Universidad Veracruzana en Xalapa.

Referencias

[1] Brown Ezra. *Three Connections to Continued Fractions.* Pi Mu Epsilon Journal, **11** (2002), 353-362.

[2] Hardy G.H., Wright E.M. *An introduction to the theory of numbers.* Oxford University Press, Oxford 1979.

[3] Ireland K., M. Rosen., *A classical introduction to modern number theory.* GTM **84** Springer Verlag 1982.

[4] Mollin R.A., *Fundamental Number Theory with Applications.* CRC Press, serie Discrete Mathematics and its Applications, Boca Raton 1998.

[5] Mollin, R.A., Oseen, B., *Applications of continued fractions.* Far east J. Math. Sci. **3** (2001), no. 4, pp 673-689.

[6] Pineda-Ruelas M., Villa-Salvador G. D. *Teoría Clásica de Números.* En preparación.

[7] Sierpinski W., *Elementary theory of numbers*, Państowe Wydawnictwo Naukowe 1964.

[8] Stewart I., Tall D., *Algebraic Number Theory and Fermat's Last Theorem.* A K Peters 2002.

[9] Williams H.C., Wunderlich M.C., *On the Parallel Generation of the Residues for the Continued Fraction Factoring Algorithm.* Math. Comp. **48** no. 177 (1987), 405-423.

Particiones

Rogelio Herrera Aguirre
Universidad Autónoma Metropolitana–Azcapotzalco
Departamento de Ciencias Básicas
Av. San Pablo No. 180,
Col. Reynosa Tamaulipas
Azcapotzalco
02200 México, D.F.
rha@correo.azc.uam.mx

Resumen

Un problema básico de la teoría (elemental) de números, es contar de cuantas maneras puede obtenerse un número natural como suma de naturales, éste puede considerarse como el problema de las particiones, el cual se relaciona con aspectos de combinatoria, que involucran a los coeficientes binomiales, y con ciertas funciones, llamadas funciones generatrices.

Dentro de las posibles variantes del problema se puede considerar al cero como un sumando válido, o no hacerlo, de hecho en la notación clásica el cero se descarta como sumando [3], por otro lado se puede considerar relevante o no el orden de los sumandos. En este trabajo se plantean, entre otras, algunas de tales variantes, encontrándose diferentes fórmulas para estimar el número de tales "particiones", al final se plantean algunos trabajos a desarrollar.

1. Sumas

En esta primera sección se trabaja con "sumas" que acepten al cero como sumando válido, y para ello iniciamos con la siguiente definición.

Definición 1.1. *Sean $n, k \in \mathbb{N}$, decimos que $SO(k,n)$ es el* **número de sumas ordenadas del natural n en k sumandos** *(con cero como sumando válido), ie*

$$SO(k,n) = \#\Big\{(x_1, x_2, \ldots, x_k) \in \mathbf{N}^k \mid \sum_{i=1}^{k} x_i = n\Big\}$$

y mediante $SD(k,n)$ *denotamos el* **número de sumas desordenadas del natural** n **en** k **sumandos** *(con cero como sumando válido), ie*

$$SD(k,n) = \#\Big\{(x_1, x_2, \ldots, x_k) \in \mathbf{N}^k \mid x_1 \geq x_2 \geq \cdots \geq x_k, \sum_{i=1}^{k} x_i = n\Big\}$$

Observación 1.1 Si $n = x_1 + x_2 + \cdots + x_i + \cdots + x_j + \cdots + x_k$ es una "suma" con $x_i \neq x_j$, entonces $n = x_1 + x_2 + \cdots + x_j + \cdots + x_i + \cdots + x_k$ es la misma "suma" en el caso de sumas desordenadas, y es una "suma" diferente en el caso de sumas ordenadas, luego por suma ordenada estamos indicando aquellas sumas en las que nos importa el orden en que aparecen los sumandos, mientras que para el caso de las sumas desordenadas no tiene importancia el orden de ellos.

Observación 1.2 Sean k, n y $SO(k,n)$ como en la definición 1.1, entonces:

$$SO(1,n) = 1 \quad \& \quad SO(k,0) = 1.$$

Por otro lado tenemos:

$$SO(k,n) = \#\bigcup_{j=0}^{n}\Big\{(x_1, x_2, \ldots, x_{k-1}) \in \mathbf{N}^k \mid \sum_{i=1}^{k-1} x_i = n - j\Big\}$$

$$= \sum_{j=0}^{n} SO(k-1, n-j)$$

De lo anterior se sigue el siguiente lema:

Lema 1.1. *Sean* k,n *y* $SO(k,n)$ *como en la definición 1.1, entonces se cumple:*

$$SO(k,n) = \sum_{j=0}^{n} SO(k-1, n-j)$$

□

De este lema se sigue:

Lema 1.2. *Sean* k,n *y* $SO(k,n)$ *como en la definición 1.1, entonces se cumple:*

$$SO(k,n) = SO(k-1,n) + SO(k,n-1)$$

Demostración:

$$\begin{aligned} SO(k,n) &= \sum_{j=0}^{n} SO(k-1,n-j) \\ &= SO(k-1,n) + \sum_{j=1}^{n} SO(k-1,n-j) \\ &= SO(k-1,n) + \sum_{t=0}^{n-1} SO(k-1,(n-1)-t) \\ &= SO(k-1,n) + SO(k,n-1) \end{aligned}$$

□

Con la ayuda de la observación 1.2 y el lema 1.2, podemos construir la siguiente tabla para $SO(k,n)$.

$k \setminus n$	0	1	2	$\cdots$	n-1	n
1	1	1	1	$\cdots$	1	1
2	1	2	3	$\cdots$	n	n+1
3	1	3	6	$\cdots$	$\frac{n(n+1)}{2}$	$\frac{(n+1)(n+2)}{2}$
4	1	4	10	$\cdots$	$\frac{n(n+1)(n+2)}{6}$	$\frac{(n+1)(n+2)(n+3)}{6}$
5	1	5	15	$\cdots$	$\frac{n(n+1)(n+2)(n+3)}{24}$	$\frac{(n+1)(n+2)(n+3)(n+4)}{24}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
k-1	1	k-1	$\frac{(k-1)k}{2}$	$\cdots$	$SO(k-1,n-1)$	$SO(k-1,n)$
k	1	k	$\frac{k(k+1)}{2}$	$\cdots$	$SO(k,n-1)$	$SO(k,n)$

Tabla 1.1 Número de Sumas Ordenadas de n en k sumandos.

De la tabla anterior se puede proponer el siguiente lema.

Lema 1.3. *Sean k,n y $SO(k,n)$ como en la definición 1.1, entonces se cumple:*

$$SO(k,n) = \binom{n+k-1}{k-1}$$

Demostración:
En efecto de la tabla se tiene que :

$$SO(1,n) = \binom{n}{0}, \quad SO(2,n) = \binom{n+1}{1}, \quad SO(3,n) = \binom{n+2}{2}, \quad etc.$$

lo cual da la base para una demostración por inducción, cuyo paso inductivo se sigue de las siguientes identidades:

$$\begin{aligned} SO(k,n) &= SO(k-1,n) + SO(k,n-1) \\ &= \tbinom{n+(k-1)-1}{(k-1)-1} + \tbinom{(n-1)+(k-1)}{k-1} \\ &= \tbinom{n+k-1}{k-1} \end{aligned}$$

□

Para poder encontrar resultados análogos a los anteriores, en el caso de sumas desordenadas procederemos a realizar el análisis de un ejemplo, que además permite reconocer la relación de los conceptos definidos, con problemas de combinatoria.

Ejemplo. Considere que entre tres individuos: Luis, Mario y Nicolás, reúnen diez pesos, sin que ninguno pueda aportar fracciones de peso, ¿de cuántas maneras puede conseguirse este resultado?.

Para responder a la pregunta revisamos la siguiente tabla:

L	M	N		
10	0	0	→	3
9	1	0	→	6
8	2	0	→	6
7	3	0	→	6
6	4	0	→	6
5	5	0	→	3
8	1	1	→	3
7	2	1	→	6
6	3	1	→	6
5	4	1	→	6
6	2	2	→	3
5	3	2	→	6
4	4	2	→	3
4	3	3	→	3

Tabla 1.2 Conjunto de formas para acumular diez pesos entre tres individuos.

Cada línea de la tabla anterior indica una forma en que Luis, Mario y Nicolás pueden juntar diez pesos, y cuántas formas de ese tipo existen, por ejemplo la fila ocho indica que Luis aporta siete pesos, Mario dos y Nicolás uno; y que con estos montos existen seis maneras distintas de aportación, del conjunto de individuos considerados, en consecuencia si sumamos los números anotados en la última columna, obtenemos 66 formas de conseguir los diez pesos, valor que corresponde al de $SO(3,10)$ el número de sumas ordenadas con tres sumandos y suma diez.

Observación 1.3 Se puede notar que los primeros seis tipos de combinaciones, corresponden a que Nicolás aporte cero pesos, los siguientes cuatro a que aporte uno, los tres que siguen a una aportación de dos pesos para Nicolás, y que en la última forma éste aporta tres pesos.

Observación 1.4 Por otro lado también se puede observar que cada línea de la tabla 1.2 corresponde a una suma desordenada, que en la interpretación del ejemplo analizado significaría, para la línea ocho, que no importa quien aporte siete, quien dos, y quien un peso, sino sólo que estos son los números que suman diez, de aquí que tenemos $SD(3,10) = 14$.

Observación 1.5 Otra observación de importancia sobre la tabla 1.2, se obtiene reescribiéndola como a continuación se indica:

L	M	N		
10	0	0	→	3
9	1	0	→	6
8	2	0	→	6
7	3	0	→	6
6	4	0	→	6
5	5	0	→	3
7	0	0	→	3
6	1	0	→	6
5	2	0	→	6
4	3	0	→	6
4	0	0	→	3
3	1	0	→	6
2	2	0	→	3
1	0	0	→	3

Tabla 1.3 Conjunto modificado de formas para acumular diez pesos

de donde se puede obtener la identidad siguiente:

$$SD(3,10) = SD(2,10) + SD(2,7) + SD(2,4) + SD(2,1)$$

y se propone el siguiente lema.

Lema 1.4. *Sean k, n y $SD(k,n)$ como en la definición 1.1, entonces se cumple:*

$$SD(k,n) = \sum_{j=0}^{div(n,k)} SD(k-1, n-jk)$$

Demostración:
Mostraremos primero que de cada $(a_1, a_2, \ldots, a_{k-1}) \in SD(k-1, n-jk)$ con $0 \leq j \leq div(n,k)$ se obtiene un elemento $(b_1, b_2, \ldots, b_{k-1}, b_k) \in SD(k,n)$, en efecto si $(a_1, a_2, \ldots, a_{k-1})$ es como se indicó, entonces:

$$a_1 \geq a_2 \geq \ldots \geq a_{k-1} \qquad \& \qquad \sum_{i=1}^{k-1} a_i = n - jk$$

luego definiendo:

$$b_i = a_i + j \quad \text{para} \quad i = 1, 2, \ldots, k-1 \quad \& \quad b_k = j$$

se cumple: $(b_1, b_2, \ldots, b_{k-1}, b_k) \in SD(k,n)$, puesto que:

$$b_1 \geq b_2 \geq \ldots \geq b_{k-1} \geq b_k \qquad \& \qquad \sum_{i=1}^{k} b_i = n$$

finalmente mostramos que si $(b_1, b_2, \ldots, b_{k-1}, b_k) \in SD(k,n)$, entonces existe un único $0 \leq j_0 \leq div(n,k)$ y un sólo $(a_1, a_2, \ldots, a_{k-1}) \in SD(k-1, n-j_0 k)$ de los cuales se obtiene nuestro elemento en $SD(k,n)$, indicado por medio del procedimiento anterior, para lo cual basta elegir $j_0 = b_k$, y definir:

$$a_i = b_i - j_0 \quad \text{para} \quad i = 1, 2, \ldots, k-1$$

□

Éste es un lema equivalente al lema 1.1, para las sumas ordenadas, y como en aquel caso tenemos también en consecuencia una fórmula recursiva que permite calcular $SD(k,n)$, en función de dos valores previos, como se indica a continuación:

Lema 1.5. *Sean k, n y $SD(k,n)$ como en la definición 1.1, entonces se cumple:*

$$SD(k,n) = SD(k-1, n) + SD(k, n-k)$$

Demostración:

$$\begin{aligned} SD(k,n) &= \sum_{j=0}^{div(n,k)} SD(k-1,n-jk) \\ &= SD(k-1,n) + \sum_{j=1}^{div(n,k)} SD(k-1,n-jk) \\ &= SD(k-1,n) + \sum_{t=0}^{div(n,k)-1} SD(k-1,n-(t+1)k) \\ &= SD(k-1,n) + \sum_{t=0}^{div(n-k,k)} SD(k-1,(n-k)-tk) \\ &= SD(k-1,n) + SD(k,n-k) \end{aligned}$$

□

Observación 1.6 Sean k, n y $SD(k,n)$ como en la definición 1.1, entonces se cumple:

$$SD(1,n) = SD(k,0) = SD(k,1) = 1 \quad \& \quad SD(k,t) = 0 \quad \text{si} \quad t < 0.$$

Usando la observación anterior, y el lema 5 se puede construir la siguiente tabla:

$k \setminus n$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	1	2	2	3	3	4	4	5	5	6	6	7	7	8
3	1	1	2	3	4	5	7	8	10	12	14	16	19	21	24
4	1	1	2	3	5	6	9	11	15	18	23	27	34	39	47
5	1	1	2	3	5	7	10	13	18	23	30	37	47	57	70
6	1	1	2	3	5	7	11	14	20	26	35	44	58	71	90
7	1	1	2	3	5	7	11	15	21	28	38	49	65	82	105
8	1	1	2	3	5	7	11	15	22	29	40	52	70	89	116
9	1	1	2	3	5	7	11	15	22	30	41	54	73	94	123
10	1	1	2	3	5	7	11	15	22	30	42	55	75	97	128
11	1	1	2	3	5	7	11	15	22	30	42	56	76	99	131
12	1	1	2	3	5	7	11	15	22	30	42	56	77	100	133
13	1	1	2	3	5	7	11	15	22	30	42	56	77	101	134
14	1	1	2	3	5	7	11	15	22	30	42	56	77	101	135

Tabla 1.4 Número de Sumas Desordenadas de n en k sumandos.

En este caso no tenemos una expresión sencilla para $SD(k,n)$, como la encontrada en el lema 1.3 para $SO(k,n)$, y si bien la recurrencia indicada en el lema 1.5 puede considerarse fundamental para el cálculo de los valores de $SD(k,n)$; también se pueden, con auxilio del lema 1.4 y de la observación 1.6, obtener expresiones como las siguientes:

$$
\begin{aligned}
SD(1,n) &= 1 \\
SD(2,n) &= 1 + div(n,2) \\
SD(3,n) &= 1 + div(n,3) + \sum_{j=0}^{div(n,3)} div(n-3j,2) \\
SD(4,n) &= 1 + div(n,4) + \sum_{j=0}^{div(n,4)} div(n-4j,3) \\
&\quad + \sum_{j=0}^{div(n,4)} \sum_{k=0}^{div(n-4j,3)} div(n-4j-3k,2) \\
SD(5,n) &= 1 + div(n,5) + \sum_{j=0}^{div(n,5)} div(n-5j,4) \\
&\quad + \sum_{j=0}^{div(n,5)} \sum_{k=0}^{div(n-5j,4)} div(n-5j-4k,3) \\
&\quad + \sum_{j=0}^{div(n,5)} \sum_{k=0}^{div(n-5j,4)} \sum_{t=0}^{div(n-5j-4k,3)} div(n-5j-4k-3t,2)
\end{aligned}
$$

2. Particiones

Si se revisa la tabla 1.2, presentada dentro del ejemplo de la sección anterior, uno puede considerar una variante del problema planteado, que requiera a todos los participantes aportar para reunir los diez pesos, esta variante a nivel de sumas no admite al cero como sumando válido, dando lugar a la siguiente definición:

Definición 2.1. *Sean $n,k \in \mathbf{N}$, decimos que $PO(k,n)$ es el* **número de particiones ordenadas del natural n en k sumandos** *(con cero como*

sumando válido), ie

$$PO(k,n) = \#\Big\{(x_1, x_2, \ldots, x_k) \in \mathbf{N}^k \mid x_i \geq 1,\ 1 \leq i \leq n,\ \sum_{i=1}^{k} x_i = n\Big\}$$

y mediante $PD(k,n)$ *denotamos el* **número de particiones desordenadas del natural** n **en** k **sumandos** *(con cero como sumando válido), ie*

$$PD(k,n) = \#\Big\{(x_1, \ldots, x_k) \in \mathbf{N}^k \mid x_1 \geq \cdots \geq x_k \geq 1,\ \sum_{i=1}^{k} x_i = n\Big\}$$

Observación 2.1 Sean k, n y $PO(k,n)$ como en la definición 2.1, entonces:

$$PO(1,n) = PO(n,n) = 1 \quad \& \quad PO(k,n) = 0 \quad \text{si} \quad k > n.$$

Para particiones tenemos resultados análogos a los de sumas, el correspondiente al lema 1 es:

Lema 2.1. *Sean* k,n *y* $PO(k,n)$ *como en la definición 2.1, entonces se cumple:*

$$PO(k,n) = \sum_{j=1}^{n+1-k} PO(k-1, n-j)$$

Demostración:

$$\begin{aligned} PO(k,n) &= \#\bigcup_{j=1}^{n+1-k} \Big\{(x_1, x_2, \ldots, x_{k-1}) \in \mathbf{N}^k \mid x_i \geq 1,\ 1 \leq i \leq k-1;\\ &\qquad \sum_{i=1}^{k-1} x_i = n - j\Big\}\\ &= \sum_{j=1}^{n+1-k} PO(k-1, n-j) \end{aligned}$$

□

Como en el caso de sumas, para particiones, del lema anterior se obtiene el siguiente lema.

Lema 2.2. *Sean* k,n *y* $PO(k,n)$ *como en la definición 2.1, entonces se cumple:*

$$PO(k,n) = PO(k-1, n-1) + PO(k, n-1)$$

Demostración:

$$\begin{aligned} PO(k,n) &= \sum_{j=1}^{n+1-k} PO(k-1,n-j) \\ &= PO(k-1,n-1) + \sum_{j=2}^{n+1-k} PO(k-1,n-j) \\ &= PO(k-1,n-1) + \sum_{t=1}^{(n-1)+1-k} PO(k-1,(n-1)-t) \\ &= PO(k-1,n-1) + PO(k,n-1) \end{aligned}$$

□

Ahora con ayuda de la observación 2.1 y del lema 2.2, se obtiene una tabla semejante a la tabla 1.1.

$k \setminus n$	1	2	3	4	5	.....	n-1	n
1	1	1	1	1	1	...	1	1
2	0	1	2	3	4	...	n-1	n
3	0	0	1	3	6	...	$\frac{(n-2)(n-1)}{2}$	$\frac{(n-1)n}{2}$
4	0	0	0	1	4	...	$\frac{(n-3)(n-2)(n-1)}{6}$	$\frac{(n-2)(n-1)n}{6}$
5	0	0	0	0	1	...	$\frac{(n-4)(n-3)(n-2)(n-1)}{24}$	$\frac{(n-3)(n-2)(n-1)n}{24}$
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
k-1	0	0	0	0	0	...	$PO(k-1,n-1)$	$PO(k-1,n)$
k	0	0	0	0	0	...	$PO(k,n-1)$	$PO(k,n)$

Tabla 2.1 Número de Particiones Ordenadas de n en k sumandos.

De la tabla anterior se sugiere el siguiente resultado.

Lema 2.3. *Sean k,n y $PO(k,n)$ como en la definición 2.1, entonces se cumple:*

$$PO(k,n) = \binom{n-1}{k-1}$$

Demostración:
En efecto de la tabla se tiene que :

$$PO(1,n) = \binom{n-1}{0}, \quad PO(2,n) = \binom{n-1}{1}, \quad PO(3,n) = \binom{n-1}{2}, \quad etc.$$

lo cual da la base para una demostración por inducción, cuyo paso inductivo se sigue de las siguientes identidades:

$$\begin{aligned} PO(k,n) &= PO(k-1,n-1) + PO(k,n-1) \\ &= \binom{(n-1)-1}{(k-1)-1} + \binom{(n-1)-1}{k-1} = \binom{n-1}{k-1} \end{aligned}$$

□

Para encontrar expresiones que estimen las particiones desordenadas, recuperamos del ejemplo dado, la parte de la tabla 1.2 que no permite sumandos con valor cero.

L	M	N		
8	1	1	→	3
7	2	1	→	6
6	3	1	→	6
5	4	1	→	6
6	2	2	→	3
5	3	2	→	6
4	4	2	→	3
4	3	3	→	3

Tabla 2.2 Modificación de la tabla 1.2, que no admite al cero como sumando.

En esta tabla nuevamente cada línea indica la forma de acumular diez pesos entre los tres individuos considerados, sólo que sin admitir que alguno no contribuya, anotando también de cuantas formas se puede conseguir cada una de las sumas indicadas, tomando en cuenta esto, y sumando los números anotados en la última columna obtenemos 36 como el número de formas de conseguir la suma de diez pesos por tres individuos, cada uno contribuyendo con al menos un peso y sin aportaciones fraccionarias, lo cual coincide con el valor de $PO(3,10)$.

Observación 2.2 Se tiene en este caso un comportamiento semejante al anotado en las observaciones 1.3,1.4 y 1.5, en particular se sigue que $PD(3,10) = 8$ y modificando la última tabla, se obtiene la siguiente:

L	M	N		
8	1	1	→	3
7	2	1	→	6
6	3	1	→	6
5	4	1	→	6
5	1	1	→	3
4	2	1	→	6
3	3	1	→	3
2	1	1	→	3

Tabla 2.3 Modificación de la tabla 2.2.

usada para encontrar la recurrencia de las particiones desordenadas, de donde se puede obtener la identidad siguiente:

$$PD(3,10) = PD(2,9) + PD(2,6) + PD(2,3)$$

y se propone el siguiente lema.

Lema 2.4. *Sean k, n y $PD(k,n)$ como en la definición 2.1, entonces se cumple:*

$$PD(k,n) = \sum_{j=1}^{div(n,k)} PD(k-1,(n-1)-(j-1)k)$$

Demostración:
Mostremos que de cada $(a_1, a_2, \ldots, a_{k-1}) \in PD(k-1,(n-1)-(j-1)k)$ con $1 \leq j \leq div(n,k)$ se obtiene un elemento $(b_1, b_2, \ldots, b_{k-1}, b_k) \in PD(k,n)$, en efecto si $(a_1, a_2, \ldots, a_{k-1})$ es como se indicó entonces:

$$a_1 \geq a_2 \geq \ldots \geq a_{k-1} \geq 1 \qquad \& \qquad \sum_{i=1}^{k-1} a_i = (n-1)-(j-1)k$$

luego definiendo:

$$b_i = a_i + (j-1) \quad \text{para} \quad i = 1,2,\ldots,k-1 \quad \& \quad b_k = j$$

se cumple: $(b_1, b_2, \ldots, b_{k-1}, b_k) \in PD(k,n)$, puesto que:

$$b_1 \geq b_2 \geq \ldots \geq b_{k-1} \geq b_k \geq 1 \qquad \& \qquad \sum_{i=1}^{k} b_i = n$$

finalmente mostramos que si $(b_1, b_2, \ldots, b_{k-1}, b_k) \in PD(k,n)$, entonces existe un único $1 \leq j_0 \leq div(n,k)$ y un sólo $(a_1, a_2, \ldots, a_{k-1}) \in PD(k-1,(n-1)-(j_0-1)k)$ de los cuales se obtiene nuestro elemento en $PD(k,n)$, indicado por medio del procedimiento anterior, para lo cual basta elegir $j_0 = b_k$, y definir:

$$a_i = b_i - (j_0 - 1) \quad \text{para} \quad i = 1,2,\ldots,k-1$$

□

Nuevamente como en el caso de sumas, tenemos una fórmula recursiva para $PD(k,n)$, en función de dos valores previos, como lo muestra el siguiente lema.

Lema 2.5. *Sean k, n y $PD(k,n)$ como en la definición 2.1, entonces se cumple:*

$$PD(k,n) = PD(k-1,n-1) + PD(k,n-k)$$

Demostración:

$$\begin{aligned}
PD(k,n) &= \sum_{j=1}^{div(n,k)} PD(k-1,(n-1)-(j-1)k) \\
&= PD(k-1,n-1) + \sum_{j=2}^{div(n,k)} PD(k-1,(n-1)-(j-1)k) \\
&= PD(k-1,n-1) + \sum_{t=1}^{div(n,k)-1} PD(k-1,(n-1)-tk) \\
&= PD(k-1,n-1) \\
&\quad + \sum_{t=1}^{div(n-k,k)} PD(k-1,(n-k-1)-(t-1)k) \\
&= PD(k-1,n-1) + PD(k,n-k)
\end{aligned}$$

□

Observación 2.3 Sean k, n y $PD(k,n)$ como en la definición 2.1, entonces se cumple:

$$PD(1,n) = PD(n,n) = 1 \quad \& \quad PD(k,n) = 0 \quad \text{si} \quad k > n$$

Usando la observación anterior, y el lema 2.5 se puede construir la siguiente tabla:

$k \setminus n$	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	0	1	1	2	2	3	3	4	4	5	5	6	6	7
3	0	0	1	1	2	3	4	5	7	8	10	12	14	16
4	0	0	0	1	1	2	3	5	6	9	11	15	18	23
5	0	0	0	0	1	1	2	3	5	7	10	13	18	23
6	0	0	0	0	0	1	1	2	3	5	7	11	14	20
7	0	0	0	0	0	0	1	1	2	3	5	7	11	15
8	0	0	0	0	0	0	0	1	1	2	3	5	7	11
9	0	0	0	0	0	0	0	0	1	1	2	3	5	7
10	0	0	0	0	0	0	0	0	0	1	1	2	3	5
11	0	0	0	0	0	0	0	0	0	0	1	1	2	3
12	0	0	0	0	0	0	0	0	0	0	0	1	1	2
13	0	0	0	0	0	0	0	0	0	0	0	0	1	1
14	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Tabla 2.4 Número de Particiones desordenadas de n en k sumandos.

Nuevamente en este caso no tenemos una expresión sencilla para $PD(k,n)$, como la encontrada en el lema 2.3 para $PO(k,n)$, pero también con la fórmula indicada en el lema 2.4, que puede considerarse fundamental para el cálculo de los valores de $PD(k,n)$, y con el auxilio de la observación 2.3 se obtienen expresiones como las siguientes:

$$PD(1,n) = 1$$

$$PD(2,n) = \sum_{j=1}^{div(n,2)} PD(1,n+1-2j) = div(n,2)$$

$$PD(3,n) = \sum_{t=1}^{div(n,3)} PD(2,n+2-3t) = \sum_{t=1}^{div(n,3)} div(n+2-3t,2)$$

$$PD(4,n) = \sum_{m=1}^{div(n,4)} PD(3,n+3-4m)$$

$$= \sum_{m=1}^{div(n,4)} \sum_{t=1}^{div(n+3-4m,3)} div(n+5-4m-3t,2)$$

$$PD(5,n) = \sum_{r=1}^{div(n,5)} PD(4,n+4-5r)$$

$$= \sum_{r=1}^{div(n,5)} \sum_{m=1}^{div(n+4-5r,4)} \sum_{t=1}^{div(n+7-5r-4m,3)} div(h,2)$$

donde $h = n + 9 - 5r - 4m - 3t$.

3. Propuestas a desarrollar

El presente trabajo tiene como origen una plática presentada, en el Segundo Taller de Teoría de Números del Centro–Sureste, en abril de 2007, en particular dicha exposición, se dirigió a los alumnos de la Licenciatura en Matemáticas, a cargo de la Facultad de Matemáticas de la Universidad Veracruzana, es por ello que a continuación se presentan dos propuestas a desarrollar como posibles trabajos de tesis, que si bien están pensados para los estudiantes primero mencionados, también pueden ser desarrollados por los alumnos de la Maestría en Matemáticas Educativas de la misma facultad.

Propuesta 1. Desarrollar un análisis detallado de las expresiones encontradas para sumas y particiones, usando en su caso la herramienta de las funciones generatrices, para encontrar más relaciones entre estos objetos.

Propuesta 2. Aplicar los conceptos de "sumas" y "particiones", en sus diferentes variantes, a problemas de aplicación en combinatoria; cabe anotar que en [1] se presentan problemas de aplicación a la Física, y que en el trabajo que también presenta Anzaldo, en este volumen, existen más aplicaciones al respecto.

Referencias

[1] Anzaldo M., A., Partciones de números enteros y las densidades de niveles, Memorias Primer Taller de Teoría de Números del Centro-Sureste, 2006.

[2] Grosswald, E., Topics from the Theory of Numbers, 2nd ed, Birkhauser.

[3] Hall Jr., M., Combinatorial Theory, Ginn Blaisdell, 1967.

[4] Hardy & Wright, An introducction to the theory of numbers, Oxford University Press, 1979.

Clasificación y Bases de Álgebras de Lie Nilpotentes en Sistemas Dinámicos

Alfonso Anzaldo Meneses

Universidad Autónoma Metropolitana–Azcapotzalco
Departamento de Ciencias Básicas
Av. San Pablo No. 180,
Col. Reynosa Tamaulipas
Azcapotzalco
02200 México, D.F.
alfons_rex@hotmail.com

Resumen

En el estudio de ciertos sistemas dinámicos es de gran utilidad introducir conjuntos de campos vectoriales sujetos a restricciones específicas. Así por ejemplo, un cierto campo vectorial X aplicado a un punto q del espacio de soluciones nos llevará a otro punto $q' = X(q)$, también en el espacio de soluciones, o bien en otro subespacio de interés, siempre y cuando se satisfagan ciertas condiciones. Dichas restricciones dependen de las características del modelo físico o matemático particular. En especial, se han encontrado de gran utilidad a las álgebras de Lie $\mathfrak{g}$ con base $\{X_i | i = 1, \ldots, N\}$, para $N \geq 3$, que satisfacen $\mathfrak{g}_n$, para $n > 1$, siendo $\mathfrak{g}_{i+1} = [\mathfrak{g}_0, \mathfrak{g}_i]$, $i = 0, 1, \ldots$, con $\mathfrak{g}_0 = \mathfrak{g}$. Esto es, álgebras de Lie nilpotentes de n pasos cuya estructura está limitada por las propiedades del paréntesis de Lie: $[X, Y] = -[Y, X]$ y la identidad de Jacobi $[X, [Y, Z]] + [Y, [Z, X]] + [Z, [X, Y]] = 0$. Es deseable clasificar a dichas álgebras, ya que eso permitiría entender mejor a los sistemas dinámicos asociados. Sin embargo la clasificación de las álgebras de Lie nilpotentes es un problema abierto de gran dificultad. No obstante para ciertas álgebras de Lie nilpotentes hemos podido obtener no sólo las dimensiones de sus bases sino construir igualmente a dichas bases en forma explícita. En éste trabajo utilizamos métodos elementales de teoría de números (funciones generadoras por ejemplo) que nos permiten alcanzar dicho objetivo para aquellas álgebras que además son solubles con longitud soluble dos, las cuales son aquellas tales que $[[\mathfrak{g}, \mathfrak{g}], [\mathfrak{g}, \mathfrak{g}]] = 0$. Se da una presentación elemental que sirve como introducción al estudio de sistemas dinámicos, álgebras de Lie y problemas de enumeración y clasificación de conjuntos de cierta complejidad.

1. Introdución

Sea $\mathcal{M}$ una variedad diferencial de n dimensiones y $T\mathcal{M}$ su haz tangente. La bandera de Lie derivada[1] $\Delta^{(i)}$ para la distribución $\Delta \subset T\mathcal{M}$ está definida como

$$\Delta^{(i+1)} = \Delta^{(i)} + [\Delta^{(i)}, \Delta^{(i)}], \quad \text{con} \quad \Delta^{(0)} = \Delta.$$

Definamos además a la bandera 'central' de Lie

$$\Delta^{i+1} = \Delta^{i} + [\Delta^{0}, \Delta^{i}], \quad \text{con} \quad \Delta^{0} = \Delta.$$

En general ambas banderas son distintas. Una distribución es llamada *generadora por paréntesis* si para cada $p \in \mathcal{M}$, existe un entero positivo m para el cual $\Delta_p^{(m)} = T_p\mathcal{M}$.

A partir de la sección tres se asumirá adicionalmente que $\mathfrak{g}$ es nilpotente con orden de nilpotencia M, esto es $\mathrm{ad}_{X_i}^k(X_j) = 0$, para todo $k > M$ y $X_i, X_j \in \mathfrak{g}$. Hay espacio graduado asociado a la bandera derivada $V(T_p\mathcal{M}) = N_1 \oplus N_2 \oplus \cdots \oplus N_M$, con $N_j = \Delta_p^{(j)}/\Delta_p^{(j-1)} = [\Delta^{(j-1)}, \Delta^{(j-1)}]_p$. El mapeo $V_i \times V_j \mapsto N_{i+j}$ está bien definido y este espacio vectorial esta provisto de una estructura natural de un álgebra de Lie nilpotente *graduada*.

2. Ecuaciones de Euler-Lagrange para campos analíticos

Estudiamos un sistema dinámico no lineal dado por una distribución Δ de campos vectoriales reales X_i para $i = 1, \ldots, n$ involucrados en el sistema no integrable de Pfaff

$$\dot{q} = \sum_i u_i X_i(q). \tag{1}$$

Aquí $q = (x, y)^T$, siendo x un vector n–dimensional con $\dot{x} = u$ y

$$\dot{y} = \sum_i u_i \xi_i(x),$$

[1]Recordar que la serie derivada de un álgebra de Lie g está definida por $g \supseteq g' = [g, g] \supseteq g'' = [g', g'] \supseteq \cdots \supseteq g^{(k)} = [g^{(k-1)}, g^{(k-1)}] \supseteq \cdots$. Además la serie central inferior es $g \supseteq g^2 = g' = [g, g] \supseteq g^3 = [g^2, g] \supseteq \cdots \supseteq g^k = [g^{k-1}, g] \supseteq \cdots$. El álgebra es llamada **nilpotente** si $g^k = 0$ para cierta $k > 0$, y **soluble** si $g^{(k)} = 0$ para cierta $k > 0$, entonces si g es nilpotente es soluble, pero el inverso no necesita ser válido.

con funciones analíticas reales $\xi_i(x)$. Entonces,

$$X_i = \frac{\partial}{\partial x_i} + \xi_i \frac{\partial}{\partial y}.$$

Para uso posterior hagamos

$$X_{ij} := [X_i, X_j] = F_{ij} \frac{\partial}{\partial y}, \quad i, j = 1, \ldots, n,$$

con los elementos de matriz antisimétricos

$$F_{ij} = \frac{\partial}{\partial x_j}\xi_i - \frac{\partial}{\partial x_i}\xi_j.$$

Es fácil verificar la identidad de Jacobi para los campos en Δ

$$\partial_i F_{jk} + \partial_j F_{ki} + \partial_k F_{ij} = 0.$$

Notemos que dado que dado que los ξ_j no dependen de y, todos los campos $\mathrm{Ad}_{X_{i_1}} \mathrm{Ad}_{X_{i_2}} \cdots \mathrm{Ad}_{X_{i_k}}(X_j)$ para $k > 0$ conmutan entre ellos. En consecuencia, las banderas de Lie derivada y central definidas arriba coinciden, $\Delta^{(i)} = \Delta^i$. Además, el álgebra resultante es *filtrada*[2] dado que $\Delta^{(i)} \subseteq \Delta^{(j)}$ si $i \leq j$, $g = \bigcup_i \Delta^{(i)}$ y $[\Delta^{(i)}\Delta^{(j)}] \subseteq \Delta^{(i+j)}$. Definiendo a la serie central inferior $\Delta_i = [\Delta, \Delta_{i-1}]$, para $\Delta_0 = \Delta$, el álgebra es *graduada* con $\mathfrak{g} = \sum_{i \geq 0} \oplus \Delta_i$ y $\Delta^i = \sum_{j=0}^{i} \Delta_j$. De acuerdo a ello, las partes de Δ_i son llamadas *homogéneas de grado i.*

La identidad de Jacobi limita al número de campos vectoriales linealmente independientes generados por estas banderas. Si todos los campos están en Δ la identidad es la relación dada más arriba. Pero dado que para mas de un campo en Δ_l para $l \geq 1$, la identidad es trivial, solo para dos campos en Δ, digamos X_i y X_j, y $X \in \Delta_l$ da un resultado no trivial

$$[X_i, [X_j, X]] = [X_j, [X_i, X]].$$

---

[2]Un álgebra de Lie g es graduada si $g = \sum_{i=0}^{\infty} \oplus g_i$, en donde g_i es un subespacio y $g_i g_j \subseteq g_{i+j}$. Un álgebra de Lie es filtrada si para cada entero no negativo i está definido un subespacio $g^{(i)}$ tal que (1) $g^{(i)} \subseteq g^{(j)}$ si $i \leq j$; (2) $\cup g^{(i)} = g$; (3) $g^{(i)} g^{(j)} \subseteq g^{(i+j)}$. Si existe un subespacio de $\mathfrak{g}$ que lo genera, entonces hay un filtrado dado por $g^{(i)} = \emptyset 1 + \Delta + \cdots + \Delta^i$, donde Δ^i es el subespacio generado por todos los productos de i elementos tomados de Δ.

Definamos los campos

$$X_{ij,\kappa} = \mathrm{Ad}_{X_{\kappa_r}} \mathrm{Ad}_{X_{\kappa_{r-1}}} \cdots \mathrm{Ad}_{X_{\kappa_1}}(X_{ij}), \quad \kappa = (\kappa_1, \ldots, \kappa_{r-1}, \kappa_r), \quad r \geq 1,$$

con enteros $\kappa_j = 1, 2, \ldots$. Entonces la identidad de Jacobi da

$$X_{ij,\kappa} = X_{ij,\kappa'}, \quad \kappa' = (\kappa_1, \kappa_2, \ldots, \kappa_r, \kappa_{r-1}).$$

Permitámonos notar que hay en general $n^r\, n(n-1)/2$ campos $X_{ij,\kappa}$, y que muchos de ellos podrían no ser linealmente independientes.

Para campos vectoriales analíticos en general el álgebra de Lie resultante podría ser infinita. En este trabajo hacemos la siguiente.

Suposición. La distribución Δ es generadora por paréntesis, esto es, tal que $\Delta_p^{(m)} = T_p\mathcal{M}$ para cierto entero $m > 0$.

Entonces los campos vectoriales deben conducir a álgebras de Lie *finitas*.

Sea G el grupo de Lie asociado con el álgebra de Lie generada por Δ de tal forma que los X_i sean los campos vectoriales *invariantes por la izquierda*. Para cada $q \in G$ definimos para cada plano $\Delta(q) = \mathrm{span}\{X_1, \ldots, X_n\}$ un producto interno $\langle \cdot, \cdot \rangle_{\Delta(q)}$ declarando a los vectores $\{X_i(q)\}$ ortonormales. El problema geodésico subRiemanniano sobre G, consiste aquí esencialmente en la minimización de la acción de energía cinética

$$S_0 = \frac{1}{2} \int \|\dot{q}(t)\|^2\, dt,$$

en la clase de curvas horizontales. Dichas curvas están definidas por curvas absolutamente contínuas $q : [0, t_q] \mapsto G$, siempre y cuando $\dot{q}(t) \in \Delta(q)$, casi en todas partes.

El método variacional estándar consiste en el estudio del Lagrangiano

$$L = \frac{\lambda_0}{2} \sum_i \ddot{x}_i^2 + \lambda(\dot{y} - \sum_i \xi_i \dot{x}_i).$$

El caso para el cual $\lambda_0 = 0$ es llamado anormal o singular. Para $\lambda_0 \neq 0$, tenemos el caso normal para el cual podemos tomar $\lambda_0 = 1$. Las ecuaciones de Euler-Lagrange para las normales son

$$\ddot{x} = \lambda F \dot{x}, \quad \dot{\lambda} = 0,$$

con la matriz antisimétrica F con elementos F_{ij}. Claramente, el parámetro de Lagrange λ es una constante del movimiento.

2.1. Estructuras graduadas para campos vectoriales polinomiales

Como se mencionó en la sección anterior estamos interesados en distribuciones que sean generadoras por paréntesis. Esto se puede lograr genéricamente analizando a desarrollo en series de Taylor alrededor del origen

$$\xi_j(x) = \sum_{i_1,\ldots,i_n \geq 0} \frac{1}{i_1! i_2! \cdots i_n!} \frac{\partial^{i_1}}{\partial x_{i_1}} \cdots \frac{\partial^{i_n}}{\partial x_{i_n}} \xi_j(x)\Big|_{x=0} x_1^{i_1} \cdots x_n^{i_n}.$$

Como mostraremos, este enfoque conduce al estudio de una estructura graduada introducida por Brockett y Dai (1986), llamada por ellos 'jerarquía', para analizar efectos no lineales. Brockett y Dai consideran campos vectoriales *polinomiales* X_i, que pueden ser vistos, por ejemplo, como aproximaciones a campos analíticos dadas por series de Taylor truncadas, suponiendo que las correspondientes series existen, o bien como un problema en sí mismo. Claramente si las ξ_i son polinomios, el álgebra resultante es finita como se requiere. Además $\mathfrak{g}$ será nilpotente de orden de nilpotencia m (esto es de $m+1$ pasos), dado que entonces $\Delta_k = 0$ para toda $k > m$. Aquí se propone un método libre de coordenadas para estudiar este problema.

Consideramos un enfoque general que conduce de manera natural al problema de la clasificación de las clases de isomorfismos de álgebras de Lie nilpotentes finitas. Adicionalmente, nuestros resultados proporcionan un método libre de coordenadas para estudiar ciertos sistemas dinámicos no lineales. Consideramos una distribución Δ de dimensión n, como la dada anteriormente, pero con funciones polinomiales generales ξ_i de grado m. Denotemos al álgebra generada por Δ como $\mathfrak{g}$. Esta álgebra de Lie es filtrada, graduada (recordemos que $\Delta^{(i)} = \sum_{j=0}^{i} \Delta_j$), y nilpotente de $m+1$ pasos. Además $\mathfrak{g}$ tiene longitud soluble dos, esto es $\mathfrak{g}_{(2)} = 0$. La antisimetría del paréntesis de Lie junto con la identidad de Jacobi implican que no todos los conmutadores pueden ser linealmente independientes. Una formulación genérica del problema para álgebras de Lie nilpotentes habrá sido lograda una vez que sea dada una base para los conmutadores de manera explícita. Ya que entonces el grupo conexo de Lie asociado puede ser obtenido por medio de un mapeo exponencial y la fórmula de BCH y se pueden introducir coordenadas privilegiadas para dar una base canónica para los campos vectoriales invariantes.

Lema 2.1. *El número de campos vectoriales en* Δ_r *es* $D_{n,r} = r\binom{n+r-1}{r+1}$ *para* $r > 0$. *Además, el álgebra de Lie* $\mathfrak{g}$ *tiene dimensión*

$$n+1+D_{n+1,m}-\binom{n+m}{m}.$$

Demostración:
Está claro que después de m paréntesis el campo resultante es central. Dado que los campos de distintas profundidades son linealmente independientes, las dimensiones de los subespacios Δ_r pueden ser calculados directamente considerando a la identidad de Jacobi como sigue. Supongamos que hay $D_{n,m-2}$ campos X de profundidad $m-1$ para $m \geq 2$. Estos producen entonces $n D_{n,m-2}$ campos $[X_i, X]$ de profundidad m. Sin embargo, hay $n(n-1)/2$ identidades de Jacobi, $[X_j,[X_i,X']] = [X_i,[X_j,X']]$, para cada una de los $D_{n,m-3}$ campos X' de profundidad $m-2$, relacionando campos de profundidad m, los cuales deben de ser sustraídos. Pero nuevamente, debemos considerar las $n(n-1)(n-2)/3!$ identidades de Jacobi

$$[X_j,[X_i,[X_k,X'']]] = [X_i,[X_j,[X_k,X'']]] = [X_i,[X_k,[X_j,X'']]],$$

que deben ser satisfechas por cada uno de los $D_{n,m-4}$ campos X'' de profundidad $m-3$, y los cuales deben entonces de ser restados de aquellas identidades relacionando campos de profundidad $m-2$, y con esto adicionados a la suma total. Y así siguiendo el mismo razonamiento, la fórmula general de recurrencia es

$$\sum_{k=0}^{m}(-)^k\binom{n}{k}D_{n,m-k-1}=0, \quad m \geq 2,$$

con condiciones iniciales $D_{n,0} = 0$, dado que no hay relaciones de Jacobi de solo dos términos relacionando campos de profundidad m y conteniendo solo m campos de Δ, $D_{n,-1} = -1$, debido a la identidad con m campos en Δ y finalmente $D_{n,-s} = 0$, $s > 1$, dado que no hay relaciones mas profundas. La solución de la fórmula es efectivamente $D_{n,m}$, como ha sido dada, lo cual puede demostrarse deduciendo primero la función generadora $(n-1/x)/(1-x)^n$ para las $D_{n,m}$. La dimensión del álgebra puede ser obtenida utilizando la identidad

$$\sum_{k=0}^{m}\binom{n+k-1}{k}=\binom{n+m}{m}.$$

□

Notemos la diferencia con la fórmula de dimensión de Witt para la dimensión de $\Delta_{\rho-1}$ para álgebras de Lie *libres*[9] para $r \geq 3$, dada por

$$\frac{1}{\rho}\sum_{i|\rho} \mu(\rho/i)\, n^i,$$

en donde $\mu(n)$ es la función de Möbius (es cero si la descomposición de n tiene primos repetidos, uno si $n = 1$ y $(-1)^k$ si n es el producto de k primos distintos). Las primeras dimensiones coinciden con $D_{n,1} = n(n-1)/2$ y $D_{n,2} = n(n^2-1)/3$, como puede comprobarse fácilmente. Para profundidades mayores la diferencia resultante proviene de álgebras con longitudes solubles mayores que no consideramos en este trabajo.

Una vez que ya conocemos a la dimensión de $\mathfrak{g}$, describiremos precisamente una base de Phillip Hall [1],[11], [14], [15]. Recordemos que tales bases consisten en un conjunto totalmente ordenado $\{\mathcal{P}, \prec\}$ dado por:

1. Las X_i pertenecen a $\mathcal{P}$.
2. Si $A, B \in \mathcal{P}$ y longitud (A) <longitud (B), entonces $A \prec B$.
3. Si C no está en Δ, entonces $C \in \mathcal{P}$ si y sólo si $C = [A, B]$ con $A, B \in \mathcal{P}$, $A \prec B$ y o bien $B \in \Delta$ o $B = [D, E]$, con $D, E \in \mathcal{P}$, $D \preceq A$ y $D \prec E$.

Evidentemente en nuestro caso el orden total $\prec$ está determinado por la profundidad de los paréntesis.

Proposición 2.1. *Una base de Phillip Hall $\mathcal{P}$ para el álgebra de Lie nilpotente de $m+1$ pasos $\mathfrak{g}$ está dada de la manera siguiente.*

1. *Los n elementos de Δ y los $D_{n,1} = n(n-1)/2$ campos de profundidad dos $X_{i_1,i_2} = [X_{i_1}, X_{i_2}]$, para $i_1 < i_2$.*
2. *$X_{i_3\, i_1\, i_2} = ad_{X_{i_3}}\, ad_{X_{i_1}}\, X_{i_2}$, para $i_1 < i_2 \leq i_3$ y $X_{i_2\, i_1\, i_3} = ad_{X_{i_2}}\, ad_{X_{i_1}}\, X_{i_3}$, para $i_1 \leq i_2 < i_3$. Estos son un total de $D_{n,2} = n(n^2-1)/3$ campos linealmente independientes de profundidad tres.*
3. *Los $D_{n,r+2}$ campos de profundidad $r+3 > 3$ para $r = 1, \ldots, m-3$, $X_{ji} = ad_{X_{j_r}} \cdots ad_{X_{j_1}}\, ad_{X_{i_3}}\, ad_{X_{i_1}}\, X_{i_2}$, y $X_{ji'} = ad_{X_{j_r}} \cdots ad_{X_{j_1}}\, ad_{X_{i_2}}\, ad_{X_{i_1}}\, X_{i_3}$, con $j_1 \leq j_2 \leq \cdots \leq j_r$.*

Demostración:
Para 1., dos pasos o más, no hay restricción alguna de la identidad de Jacobi y claramente $\mathcal{P}$ está dada por Δ y X_{i_1,i_2} con $i_1 < i_2$. Hay $n(n-1)/2 = D_{n,1}$ elementos X_{ij} como se espera. Para 2., tres pasos o más, notemos que para $i_3 > i_2 > i_1$, la identidad de Jacobi para los tres campos en Δ es

$$[X_{i_3}, [X_{i_2}, X_{i_1}]] + [X_{i_2}, [X_{i_1}, X_{i_3}]] + [X_{i_1}, [X_{i_3}, X_{i_2}]] = 0.$$

Aquí los primeros dos términos (X_{i_3,i_1,i_2} y X_{i_2,i_1,i_3}) pertenecen a $\mathcal{P}$, no así el tercero X_{i_1,i_3,i_2}. Por lo cual, a esta profundidad las condiciones sobre $\mathcal{P}$ toman en cuenta a las identidades de Jacobi. Así que hay $2n(n-1)(n-2)/3!$ elementos $X_{i_3 i_1 i_2}, X_{i_2 i_1 i_3}$ para $i_1 < i_2 < i_3$ y $2n(n-1)/2$ elementos $X_{i_1 i_1 i_2}, X_{i_2 i_1 i_2}$ con $i_1 < i_2$ dando un total de $n(n^2-1)/3 = D_{n,2}$ elementos de la base de profundidad tres como se esperaba. A partir de profundidad cuatro en adelante la identidad de Jacobi no es trivial tan solo si exactamente dos campos pertenecen a Δ, en tal caso $[X_{i_2}, [X_{i_1}, X]] + [X_{i_1}, [X, X_{i_2}]] = 0$, para $i_1 < i_2$ y $X_j \prec X$ para todo $X_j \in \Delta$. Entonces, el primer término pertenece a $\mathcal{P}$ pero no el segundo. Nuevamente, la condición sobre los elementos de $\mathcal{P}$ toman en cuenta plenamente a la identidad de Jacobi para *todas* las profundidades mayores. Para profundidad $r+3 > 3$ hay dos subclases.

1. Para X_{ji} hay un solo conjunto de campos con $r+3$ subíndices distintos: $j_r > \cdots > j_1 > i_3 > i_2 > i_1$ y para $X_{ji'}$ hay $r+1$ conjuntos de campos linealmente independientes con $r+3$ subíndices distintos: $j_r > \cdots > j_2 > j_1 > i_3 > i_2 > i_1$; $j_r > \cdots > j_2 > i_3 > j_1 > i_2 > i_1$; $\cdots$; $i_3 > j_r > \cdots > j_1 > i_2 > i_1$. En esta subclase hay un total de $(r+2)\binom{n}{r+3}$ campos linealmente independientes de profundidad $r+3$.

2. En esta subclase dos o más subíndices son iguales, hay al menos una igualdad y a lo sumo $r+1$. Para X_{ji}, i_1 es siempre distinto y $j_r \geq \cdots \geq j_1 \geq i_3 \geq i_2 > i_1$. Para $X_{ji'}$ hay $r+1$ tipos de desigualdades: $j_r \geq \cdots \geq j_1 \geq i_3 > i_2 \geq i_1$, $j_r \geq \cdots \geq j_2 \geq i_3 > j_1 \geq i_2 \geq i_1$, $\cdots$, $i_3 > j_r \geq \cdots \geq j_1 \geq i_2 \geq i_1$. Ahora, s igualdades conducen a una relación con solo $r+2-s$ desigualdades y cada una corresponde a $\binom{n}{r+3-s}$ índices distintos. Pero las $s = 1, \ldots, r+1$ igualdades pueden ocurrir de $\binom{r+1}{s}$ maneras veces los $r+2$ tipos de desigualdades.

Ambas subclases dan en conjunto el número de campos vectoriales linealmente independientes de profundidad $r+3>3$ como

$$(r+2)\sum_{s=0}^{r+1}\binom{r+1}{s}\binom{n}{r+3-s}=(r+2)\binom{n+r+1}{r+3},$$

pero éste es precisamente $D_{n,r+2}$. □

Los elementos restantes de $\mathfrak{g}$ pueden ser obtenidos mediante la propiedad de antisimetría y de la identidad de Jacobi.

Bibliografía

[1] BOURBAKI N., *Lie groups and Lie algebras*, Part I, Chapters 1-3 (Hermann Publishers, Paris, France, 1975).
[2] BROCKETT R.W., Control theory and singular Riemannian geometry, *New directions in applied mathematics*, Hilton, P.J. and Young G.S. Eds. (Springer-Verlag, 1981).
[3] BROCKETT R.W. AND DAI L., Nilpotent approximations of control systems and distributions, *SIAM J. Control Optim.*, **24**, no.4, 731-736 (1986).
[4] CARATHÉODORY C., *Variationsrechnung und partielle Differentialgleichungen* (B.G. Teubner Verlag., Stuttgart, 1994).
[5] CHANDRASEKHAR S., *Plasma Physics* (The University of Chicago Press, Chicago, 1975).
[6] GAVEAU B., Principle de moindre action, propagation de la chaleur et estimées sous elliptiques sur certains groupes nilpotents, *Acta Mathematica*, **30**, 94-153 (1977).
[7] GELFAND I.M. AND FOMIN S.V., *Calculus of Variations* (Dover Publ., New York, 1991).
[8] HERMES H., Nilpotent approximations of control systems and distributions, *SIAM J. Control Optim.*, **24**, no.4, 731-736 (1986).
[9] JACOBSON N., *Lie Algebras*, Intersciences tracts in pure and applied mathematics, Number 10 (John Wiley & Sons, New York, 1962).
[10] KOBAYASHI S. AND NOMIZU K., *Foundations of Differential Geometry* (Wiley, New York, 1963).
[11] LAFFERRIERE G., SUSSMANN H., Motion planning for controllable systems without drift, *Proceedings of the IEEE Conference on robotics and automation*, Sacramento CA, April 1991, 1148-1153 (IEEE Publications, New York, 1991).
[12] MONTGOMERY R., Abnormal minimizers, *SIAM J. Control Optim.*, **32**, no. 6, 1605-1620 (1994).

[13] MONTGOMERY R., *A tour of Subriemannian geometries, their geodesics and applications*, Mathematical surveys and monographs, Vol. 91 (American Mathematical Society, 2002).

[14] VERSHIK A.M. AND GERSHKOVICH V.YA., Nonholonomic dynamical systems, geometry of distributions and variational problems. In: *Encyclopedy of Mathematical Sciences,* Vol. 16; *Dynamical systems VII* (Springer-Verlag, 1991).

[14] HALL P. "A contribution to the theory of groups of prime order", Proc. London Math. Soc. (Ser. 2) **36**,29-95 (1933).

Euler y la teoría de números

Martha Rzedowski Calderón
Cinvestav-IPN
Departamento de Control Automático
Apartado Postal 14-740,
07000 México, D.F.
mrzedowski@ctrl.cinvestav.mx

1. Biografía

Leonhard Euler nació el 15 de abril de 1707 en Basilea, Suiza, fue hijo de Paul Euler, pastor protestante, y de Margarita Brucker, también hija de un pastor, tuvo dos hermanas más jóvenes que él nombradas Ana Maria y Maria Magdalena. Su padre había asistido a las clases de matemáticas impartidas por Jacob Bernoulli. A la edad de trece años Leonhard se matriculó en la Universidad de Basilea, y en 1723, se graduó con una disertación que comparaba las filosofías de Descartes y de Newton. En este tiempo, recibía lecciones en la tarde del sábado de Johann Bernoulli (hermano menor de Jacob), quien descubrió rápidamente el talento increíble para las matemáticas de su pupilo.

Euler estudiaba teología, pero Johann Bernoulli intervino, y convenció a Paul Euler de que Leonhard estaba destinado a ser un gran matemático. En 1726, Euler terminó su tesis doctoral en la propagación del sonido. En 1727 participó en la competencia de la Academia de París, el problema del año era encontrar la mejor manera de colocar los mástiles en una nave. Euler obtuvo el segundo lugar, perdiendo solamente ante Pierre Bouguer (conocido actualmente como "el padre de la arquitectura naval"). Sin embargo, Euler eventualmente ganaría dicho premio anual en doce ocasiones.

Alrededor de este tiempo, los hijos de Johann Bernoulli, Daniel y Nicolas trabajaban en la Academia de Ciencias Imperial Rusa en San Petersburgo. En julio de 1726, Nicolas murió de apendicitis y cuando Daniel ocupó la posición de su hermano en la división de Matemáticas y Física, él recomendó que el puesto en fisiología que él desocupó fuera llenado por su amigo Euler. En noviembre de 1726 Euler había aceptado la oferta, pero se retrasó en hacer

el viaje a San Petersburgo. En el ínterin Euler solicitó (y no tuvo éxito) un puesto en física en la Universidad de Basilea.

Euler llegó a la capital rusa en mayo de 1727. Lo promovieron de su puesto en el departamento médico de la academia a una posición en el departamento de matemáticas. Se alojó con Daniel Bernoulli, con quien a menudo tuvo una colaboración cercana. Euler dominó el idioma ruso y se adaptó a la vida en San Petersburgo. También tuvo un trabajo adicional como médico en la marina de guerra rusa.

La Academia en San Petersburgo fue establecida por Pedro el Grande para mejorar la educación en Rusia y para cerrar la brecha científica con Europa Occidental. Consecuentemente, era especialmente atractiva a los eruditos extranjeros como Euler: la academia poseía recursos financieros amplios y una extensa biblioteca. En la academia se admitía a muy pocos estudiantes pues ésta se enfocaba en la investigación.

Catalina I, quien había procurado continuar las políticas progresistas de su difunto marido, murió poco antes de la llegada de Euler. Esto causó muchas dificultades para Euler y sus colegas. Las condiciones mejoraron levemente después de la muerte de Pedro II. Euler progresó rápidamente en las filas de la academia y fue hecho profesor de física en 1731. Dos años más tarde, Daniel Bernoulli emigró para Basilea y Euler ocupó su puesto en matemáticas.

En 1734 contrajo matrimonio con Katharina Gsell, hija de un pintor del gimnasio de la academia. Compraron una casa por el Río Neva y tuvieron trece hijos, de los cuales solamente cinco vivieron más allá de la infancia.

Preocupado por la continua agitación en Rusia, Euler se preguntaba si permanecer en San Petersburgo o no. Federico el Grande de Prusia le ofreció un puesto en la Academia de Berlín, mismo que él aceptó. Dejó San Petersburgo en 1741 y vivió por veinticinco años en Berlín, en donde escribió más de 380 artículos.

Se le pidió a Euler que fuera profesor particular de la princesa de Anhalt-Dessau, sobrina de Federico. Le escribió más de 200 cartas, mismas que fueron compiladas en un volumen de gran éxito (best seller) titulado Cartas de Euler en Diversos Temas de Filosofía Natural a una Princesa Alemana. Este trabajo contiene la exposición de Euler en varios temas que pertenecen a la física y a las matemáticas y ofrece valiosa información acerca de la personalidad y las creencias religiosas de Euler. Este libro ha sido más

leído que cualquiera de sus trabajos matemáticos. Su popularidad atestigua la capacidad de Euler para comunicar eficazmente temas científicos a no especialistas.

A pesar de la inmensa contribución de Euler al prestigio de la academia, eventualmente fue forzado a salir de Berlín. Esto fue causado en parte por un conflicto de personalidad con Federico, quien lo veía como falto de sofisticación, especialmente en comparación al círculo de filósofos que el rey alemán había llevado a la academia. Voltaire estaba entre ellos y gozaba de una posición favorable. Euler, hombre religioso y simple y trabajador duro, era muy convencional en sus creencias y gustos. Era, en muchos sentidos, lo opuesto a Voltaire. Euler estaba poco entrenado en retórica y tendía a discutir sobre temas de los que sabía poco, siendo blanco del ingenio de Voltaire. Además Federico expresó su decepción ante las capacidades prácticas de ingeniería de Euler.

Tres años después de sufrir una fiebre casi fatal en 1735, Euler perdió casi totalmente la vista de su su ojo derecho, pero él más bien culpó de su condición al meticuloso trabajo de cartografía que realizó para la Academia de San Petersburgo. La vista de Euler en ese ojo empeoró a través de su estancia en Alemania, tanto que Federico se refería a él como "cíclope". Más adelante Euler sufrió una catarata en su ojo izquierdo, quedando casi totalmente ciego poco tiempo después. Su condición pareció tener poco efecto en su productividad, pues la compensó con sus habilidades mentales de cálculo y memoria. Por ejemplo, Euler podía repetir la Eneida de Virgilio de principio a fin sin vacilación.

La situación en Rusia había mejorado notablemente desde la ascensión de Catalina la Grande, y en 1766 Euler aceptó una invitación de volver a la Academia de San Petersburgo y pasó el resto de su vida en Rusia. Un fuego en 1771 en San Petersburgo le costó su hogar. En 1773, perdió a su esposa de 40 años. Volvió a casarse en 1776, con Salome Abigail Gsell, media hermana de su primera esposa.

Cuando tenía 19 años, J. L. Lagrange (1736–1813) escribió una carta a Euler, en la cual solucionaba el problema isoperimétrico que por más de medio siglo había sido un tema de discusión. Para obtener la solución enunció los principios del cálculo de variaciones.

Euler reconoció la generalidad del método adoptado, y su superioridad respecto al usado por él mismo; y con su cortesía característica retuvo un

artículo que había escrito previamente, el cual cubría algo del mismo tema, para que el joven italiano pudiera tener tiempo para terminar su trabajo, y recibir el crédito por el nuevo cálculo. El nombre de esta rama del análisis fue sugerido por Euler. Este trabajo colocó a Lagrange inmediatamente en primer plano entre los matemáticos vivos en ese entonces.

Nicolaus Fuss (1755–1826) nació y fue educado en Basilea, Suiza. Debido en parte a su entrenamiento matemático, Daniel Bernoulli le recomendó como asistente/secretario para el casi ciego Euler. Fuss llegó a San Petersburgo en 1773 y ayudó a Euler a preparar más de 250 artículos. Se casó con la primera hija del también matemático Johann Albrecht Euler (1734–1800), hijo mayor de Leonhard. Además de haber sido académicos ellos mismos, J. A. Euler y Nicolaus Fuss, ayudaron de muchas maneras a continuar el gran legado de Euler.

El 7 de septiembre de 1783, Euler murió en San Petersburgo después de sufrir una hemorragia cerebral. Fue enterrado en el Alexander Nevsky Laura. Su panegírico fue escrito para la Academia Francesa por el matemático y filósofo francés Marqués de Condorcet y un recuento de su vida, con una lista de sus trabajos por Nicolaus Fuss. Condorcet comentó:

"... a il cessa de calculer et de vivre"

(cesó él de calcular y de vivir)

Tomado principalmente de: http://en.wikipedia.org/wiki/Leonhard_euler (Wikipedia)

2. Carácter y estilo personal

Los contemporáneos y los biógrafos de Euler coinciden en la valoración de su carácter: tenía una naturaleza abierta y alegre; era sencillo, de buen humor y sociable. Aunque próspero y aun rico - por lo menos en la segunda mitad de su vida - con respecto a cosas materiales era absolutamente modesto. Libre de toda arrogancia, nunca guardaba un resentimiento, con todo al mismo tiempo era seguro de sí mismo, crítico, y "atrevido". Aunque puede ser que de vez en cuando perdiera los estribos, era solamente por unos breves momentos, después de lo cual se disolvería inmediatamente en risa otra vez. Las demandas científicas de propiedad de autor le eran también extranjeras a Euler; a diferencia de la mayoría de los eruditos y de los artistas a través de la historia, él nunca se enganchó en conflictos sobre derechos

de autor; antes el contrario, dio de vez en cuando generosamente nuevos descubrimientos y conocimiento. El trabajo de Euler no oculta nada; pone siempre sus cartas sobre la mesa, ofreciendo al lector las mismas condiciones y oportunidades de encontrar algo nuevo. Él incluso a menudo conduce al lector muy cerca del descubrimiento, pero le deja la alegría de descubrirlo. Esta educación genuina hace de los libros de Euler una experiencia de aprendizaje que anima y entretiene. Parece haber sido incapaz de sentir envidia; nunca envidió nada a nadie y estaba siempre encantado con los descubrimientos de otros, como su correspondencia lo demuestra en cientos de casos. Todo esto fue posible debido a sus energías intelectuales inconmensurables y a el alma inusualmente bien equilibrada de Euler.

Tomado de: http://www.leonhard-euler.ch/ (Euler Commission)

3. Aportaciones

3.1. En general

Con respecto a la disciplina, sus escritos se distribuyen aproximadamente como sigue:

Álgebra, teoría de números, análisis	40 %
Mecánica y otras partes de la física	28 %
Geometría, incluyendo trigonometría	18 %
Astronomía	11 %
Teoría de barcos, artillería, arquitectura	2 %
Filosofía, teoría de la música, teología, cualquier otra cosa no incluída arriba	1 %

Tomado de: http://www.leonhard-euler.ch/ (Euler Commission)

- En **lógica** se le atribuye el uso de curvas cerradas para ilustrar el razonamiento silogístico (1768). Dichos diagramas se conocen como diagramas de Euler.

- Uno de los intereses más inusuales de Euler era el uso de ideas matemáticas en la **música**. En 1739 escribió *Tentamen novae theoriae musicae*, esperando integrar eventualmente la teoría musical como parte de las matemáticas. Esta parte de su trabajo, sin embargo, no recibió mucha atención y fue alguna vez descrita como de-

masiado matemática para los músicos y demasiado musical para los matemáticos.

- En **física y astronomía** Euler ayudó al desarrollo de la ecuación de la viga de Euler-Bernoulli, que es una piedra angular de la ingeniería. Aparte de aplicar con éxito sus herramientas analíticas a los problemas de mecánica clásica, Euler también aplicó estas técnicas a los problemas celestes. Su trabajo en astronomía fue reconocido con un buen número de premios de la Academia de París a lo largo de su carrera. Sus logros incluyen la determinación con gran exactitud de las órbitas de cometas y de otros cuerpos celestes, el entendimiento de la naturaleza de los cometas y el cálculo del paralaje del sol. Sus cálculos contribuyeron al desarrollo de tablas de longitud precisas. Además, Euler hizo contribuciones importantes en óptica. Discrepaba con Newton acerca de la teoría corpuscular de la luz en su *Opticks*, que era la teoría que entonces prevalecía. Sus artículos de 1740 en óptica ayudaron a que la teoría ondulatoria luz propuesta por Christian Huygens se convirtiera en el modo dominante de pensamiento, por lo menos hasta el desarrollo de la teoría cuántica de la luz.

Tomado de: http://en.wikipedia.org/wiki/Leonhard_euler (Wikipedia)

3.2. En notación

- Euler introdujo y popularizó varias convenciones de escritura a través de sus numerosos y ampliamente circulados libros de texto.
- Notablemente introdujo el concepto de función y fue el primero en escribir $f(x)$ para denotar la función f aplicada al argumento x.
- También introdujo la notación moderna para las funciones trigonométricas, la letra e para la base de los logaritmos naturales (también conocida como número de Euler), la letra griega Σ para las sumatorias y la letra i para denotar la unidad imaginaria. Aunque no se originó con él, popularizó el uso de la letra griega π para denotar el cociente de la circunferencia de un círculo a su diámetro.

Tomado de: http://en.wikipedia.org/wiki/Leonhard_euler (Wikipedia)

3.3. En matemáticas

La distribución de los trabajos matemáticos de Euler es aproximadamente como sigue:

Álgebra, combinatoria y teoría de probabilidad	10 %
Teoría de números	13 %
Análisis fundamental y cálculo diferencial	7 %
Series infinitas	13 %
Cálculo Integral	20 %
Ecuaciones diferenciales	13 %
Cálculo de variaciones	7 %
Geometría, incluyendo geometría diferencial	17 %

Tomado de: http://www.leonhard-euler.ch/(Euler Commission)

- En **análisis:**
  El desarrollo del cálculo estaba en la vanguardia de la investigación matemática en el siglo XVIII y los Bernoulli eran responsables de mucho del progreso inicial en el tema. Gracias a su influencia, el estudio del cálculo se convirtió en el foco principal del trabajo de Euler. Aunque algunas de las pruebas de Euler pudieran no ser aceptables bajo los estándares modernos del rigor, sus ideas condujeron a muchos grandes avances.
  Euler es bien conocido en análisis por el uso frecuente y el desarrollo de la series de potencias: es decir, la expresión de funciones como sumas infinitas, por ejemplo:

$$e = \sum_{n=0}^{\infty} \frac{1}{n!} = \lim_{n\to\infty} \left(\frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!} \right)$$

  Euler descubrió las expresiones, como series de potencias, para e y para la función inversa de la tangente. Su uso atrevido (y, para los estándares modernos, técnicamente incorrecto) de las series de potencias le permitió solucionar el famoso Problema de Basilea en 1735:

$$\lim_{n\to\infty} \left(\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} \right) = \frac{\pi^2}{6}$$

  Euler introdujo el uso de la función exponencial y de los logaritmos en pruebas analíticas. Descubrió maneras de expresar varias funciones

logarítmicas en términos de series de potencias, y definió con éxito los logaritmos para números negativos y para números complejos, incrementando el alcance de los logaritmos en las aplicaciones en matemáticas. También definió la función exponencial para números complejos y descubrió su relación con las funciones trigonométricas. Para cualquier número real x, la fórmula de Euler indica:

$$e^{ix} = \cos x + i \operatorname{sen} x$$

Un caso especial de la fórmula anterior es conocido como la identidad de Euler:

$$e^{i\pi} + 1 = 0$$

llamada "la fórmula más notable de las matemáticas" por Richard Feynman, por su exclusivo uso de las nociones de adición, multiplicación, exponenciación e igualdad, y el sólo uso de algunos de los números más importantes, a saber: $0, 1, e, i$ y π.

- En 1736, Euler solucionó un problema conocido como "Los Siete Puentes de Königsberg". Por la ciudad de Königsberg en Prusia (ahora Kaliningrad, Rusia) pasa el Río Pregel que tiene dos islas grandes que están conectadas una con otra y con el continente a través de siete puentes. La pregunta es si es posible caminar por una ruta que cruce cada puente exactamente una vez y volver al punto de partida. No lo es; y por lo tanto no es un circuito euleriano. Esta solución se considera el primer teorema de la **teoría de gráficas**.

- Euler también introdujo la noción ahora conocida como característica de Euler y una fórmula que relaciona el número de vértices, de aristas y de caras de un poliedro convexo con esta característica

$$v - a + c = 2.$$

El estudio y la generalización de esta fórmula, específicamente por Cauchy y L'Huillier se ubica en el origen de la **topología**.

- Además, Euler elaboró la teoría de funciones trascendentes superiores introduciendo la función gamma y obtuvo un nuevo método para solucionar ecuaciones cuárticas. También encontró una manera de calcular integrales con límites complejos, presagiando el desarrollo del **análisis complejo** moderno. Le dio nombre y participó en el **cálculo de variaciones**, incluyendo su resultado mejor conocido, la ecuación de Euler-Lagrange.

- **En matemáticas aplicadas:**
  Algunos de los mayores éxitos de Euler consistieron en usar métodos analíticos para solucionar problemas del mundo real, describiendo múltiples usos de los números de Bernoulli, las series de Fourier, los diagramas de Venn, los números de Euler, las constantes e y π, las fracciones continuadas y las integrales. Integró el cálculo diferencial de Leibniz con el método de fluxiones de Newton y desarrolló las herramientas que hicieron más fácil aplicar el cálculo a los problemas físicos. Dio grandes pasos al mejorar la aproximación numérica de integrales, inventando lo que ahora se conoce como las aproximaciones de Euler. Las más notables de estas aproximaciones son el método de Euler y el fórmula de Euler-Maclaurin. También facilitó el uso de ecuaciones diferenciales, en particular introdujo la constante de Euler-Mascheroni:

$$\gamma = \lim_{n\to\infty}\left(1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots+\frac{1}{n}-\ln(n)\right)$$

Tomado de: http://en.wikipedia.org/wiki/Leonhard_euler (Wikipedia)

3.4. En teoría de números

- El gran interés de Euler en teoría de números se puede remontar a la influencia de su amigo Christian Goldbach en la Academia de San Petersburgo, pero también al interés de los Bernoulli en el tema. Muchos de sus primeros trabajos sobre teoría de números están basados en los trabajos de Pierre de Fermat. Euler desarrolló algunas de las ideas de Fermat y refutó al menos una de sus conjeturas.

- Goldbach preguntó a Euler en 1729, si sabía de la conjetura de Fermat que decía que los números de la forma $2^n + 1$ eran siempre primos si n es una potencia de 2. Euler la verificó para $n = 1, 2, 4, 8$ y 16 y, por ahí de 1732 a lo más, probó que el siguiente caso:

$$2^{32} + 1 = 4294967297$$

  es divisible entre 641 y por tanto no es primo.

- La conjetura de Goldbach es uno de los problemas no resueltos más antiguos de la de teoría de números y de todas las matemáticas. La versión "actual" nos dice:

Todo entero par mayor que 2 se puede escribir como la suma de dos primos

El 7 de junio de 1742, Christian Goldbach escribió una carta a Leonhard Euler (letter XLIII) en la cual le proponía la siguiente conjetura:

Es scheinet wenigstens, daßeine jede Zahl, die größer ist als 2, ein aggregatum trium numerorum primorum sey

Al menos parece que cada uno de los números mayores de 2 es un agregado de tres números primos

Todo entero mayor que 2 se puede escribir como suma de tres primos

observamos que Goldbach consideraba a 1 un número primo (cosa que aún ahora algunos consideran). En su libro *Vollständige Anleitung zur Algebra* (Elements of Algebra) de 1767, Euler claramente considera que 1 no es primo.

- Euler probó:
  - Las identidades de Newton
  - El Teorema Pequeño de Fermat:
    Si p es un número primo, entonces para cualquier entero a tenemos:
    $$a^p \equiv a(\text{mód}p).$$
  - El teorema de Fermat sobre sumas de dos cuadrados:
    Un número primo impar se puede expresar en la forma $p = x^2+y^2$ con x y y enteros, si y sólo si $p \equiv 1(\text{mód}4)$.
  - Otra afirmación de Fermat: que si a y b son enteros primos relativos, entonces $a^2 + b^2$ no tiene divisores de la forma $4n - 1$.
  - El caso $n = 3$ del Último Teorema de Fermat.
- Euler inventó la función φ (fi) de Euler, la cual asigna a un número entero positivo n el número de enteros positivos menores o iguales que n y primos relativos a n, denotado por $\varphi(n)$. Pudo generalizar el Teorema Pequeño de Fermat a lo que se conoce como Teorema de

Euler:
Si n es un entero positivo y a es un entero primo relativo a n, entonces:

$$a^{\varphi(n)} \equiv 1(\text{mód}n).$$

- Contribuyó a la comprensión de los números perfectos (igual a la suma de sus divisores propios, como 6), que han fascinado a los matemáticos desde tiempos de Euclides y son tema de actualidad. Euler probó que la fórmula $2^{n-1}(2^n - 1)$ provee todos los números perfectos pares.

- Euler contribuyó al Teorema de los Cuatro Cuadrados de Lagrange. Dicho teorema aparece en la aritmética de Diofanto de Bachet. Dice que todo entero positivo puede ser expresado como la suma de los cuadrados de cuatro enteros. Por ejemplo:

$$3 = 1^2 + 1^2 + 1^2 + 0^2$$
$$31 = 5^2 + 2^2 + 1^2 + 1^2$$

- Euler obtuvo la fracción continuada de e:

$$e - 1 = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6 + \ldots}}}}}}}}$$

Euler también fue pionero en el uso de métodos analíticos para solucionar problemas de la teoría de números. Al hacerlo, unió dos ramas muy distintas de las matemáticas e introdujo un nuevo campo de estudio, la teoría analítica de números. Al abrir camino para este nuevo campo, Euler creó la teoría de series hipergeométricas, las q-series, las funciones trigonométricas hiperbólicas y la teoría analítica de las fracciones continuadas. Usó métodos analíticos para obtener una cierta comprensión de la forma en que están distribuidos los números primos.

- Uno de los enfoques del trabajo de Euler era ligar la naturaleza de la distribución de los primos con ideas del análisis. Probó que la suma de los recíprocos de los primos diverge (y por tanto hay una infinidad de primos).

- Descubrió la conexión entre la función zeta de Riemann y los números primos, conocida como la fórmula del producto de Euler para la función zeta de Riemann.

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}},$$

donde ζ denota la función zeta de Riemann y el producto se extiende sobre todos los números primos p.

- Su trabajo en esta área condujo al desarrollo del teorema de los números primos:

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\ln(x)} = 1,$$

donde $\pi(x)$ cuenta los primos menores o iguales que x.

- Conjeturó la ley de reciprocidad cuadrática (probada por Gauss):

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4},$$

donde p y q son primos impares, $\left(\frac{p}{q}\right)$ es el símbolo de Legendre que es igual a 1 si p es un cuadrado módulo q y es igual a -1 en otro caso.

Tomado principalmente de: http://en.wikipedia.org/wiki/Leonhard_euler (Wikipedia)

4. Trabajos escritos

Una colección "definitiva" de los trabajos de Euler, titulada *Opera Omnia*, ha sido publicada desde 1911 por la Comisión de Euler (Euler Commission) de la Academia Suiza de Ciencias.

La distribución en el tiempo de los trabajos de Euler es aproximadamente como sigue:

Años	# de trabajos	%
1725–1734	35	5
1735–1744	50	10
1745–1754	150	19
1755–1764	110	14
1765–1774	145	18
1775–1783	270	34

Tomado de: http://www.leonhard-euler.ch/(Euler Commission)

5. El fenómeno Euler

Tres factores explican el "fenómeno Euler". Antes que nada, su, quizás única, superdotada memoria. Cualquier cosa que hubiera Euler oído, visto, pensado o escrito, él parece haberla recordado su vida entera, como incontables de sus contemporáneos atestiguarían. Podía recordar décadas más tarde las minutas de las reuniones de la academia, por no decir nada de su memoria para las cosas matemáticas. En segundo lugar, la memoria prodigiosa de Euler fue de la mano con una rara capacidad de concentración. Ruido y alboroto en su ambiente inmediato alteraban apenas su pensamiento: "un niño en sus rodillas, un gato a su espalda - así es cómo él escribió sus trabajos inmortales" divulgó Thiébault, su colega de la Academia de Berlín. El tercer factor en el "misterio de Euler" es absolutamente simple: trabajo calmado y constante.

Tomado de: http://www.leonhard-euler.ch/(Euler Commission)

6. Llevan su nombre

En matemáticas y en física hay muchos temas que llevan el nombre de Euler. Lo cual a veces ha resultado ambiguo. Euler trabajó en muchas áreas y con frecuencia es la primera referencia escrita en un tema dado. Hay la broma de que en un esfuerzo por evitar dar el nombre de Euler a un número excesivo de descubrimientos o teoremas, se les da el nombre de la primera persona que los descubrió, después de Euler. A continuación algunas de las cosas que llevan su nombre:

- Ángulos de Euler, que definen una rotación en el espacio
- Aproximación de Euler
- Asteroide Euler 2002
- Calle en la Delegación Miguel Hidalgo, por Polanco
- Característica de Euler en topología algebraica y en teoría de gráficas topológica y la fórmula de Euler correspondiente $\chi(S^2) = f - e + v = 2$, donde f es el número de caras, e es el número de aristas y v es el número de vértices de un poliedro convexo, homeomorfo a la esfera.
- Conjetura de Euler
- Constante de Euler–Mascheroni o constante de Euler $\gamma \approx 0.577216$
- Cráter en la Luna
- Cuadrados de Euler, usualmente llamados cuadrados grecolatinos
- Derivada de Euler (en oposición a derivada de Lagrange)
- Diagrama de Euler
- Disco de Euler
- Ecuación de Euler–Cauchy, una ecuación diferencial lineal de segundo orden
- Ecuación de Euler–Lagrange (en relación a problemas de minimización)
- Ecuación de Euler–Tricomi
- Ecuación de Euler, usualmente se refiere a ecuaciones de Euler, fórmula de Euler o identidad de Euler
- Ecuación de la viga de Euler-Bernoulli, referente a la elasticidad de vigas estructurales
- Ecuaciones de Euler, concernientes a rotaciones de un cuerpo rígido
- Ecuaciones de Euler en dinámica de fluidos
- Ed Sandifer's How Euler Did It

- Fórmula de Euler en análisis complejo:

$$e^{ix} = \cos x + i \operatorname{sen} x$$

- Fórmula de Euler–Maclaurin
- Función fi (φ) de Euler, cuenta el número de enteros positivos primos relativos y menores o iguales que un entero dado
- Gráfica de Euler
- Identidad de Euler:

$$e^{i\pi} + 1 = 0$$

- Integrales de Euler del primero y segundo tipo, a saber la función beta y la función gamma
- La función de Euler, una forma modular que es una q-serie prototipo
- La identidad de Euler podría también referirse al teorema de números pentagonales
- Ladrillo de Euler
- Lenguaje de programación Euler
- Medalla Euler, un premio para investigación en combinatoria
- Método de Euler
- Número de Euler, número de cavitación en dinámica de fluidos
- Número de Euler $e \approx 2.71828$, base de los logaritmos naturales, también conocido como constante de Napier
- Números de Euler (una sucesión de números enteros)
- Números idóneos de Euler
- Polinomios de Euler
- Parámetros de Euler–Rodrigues
- Portal para búsqueda de publicaciones matemáticas
- Problema de los tres cuerpos de Euler

- Productos de Euler
- Regla de Euler (para encontrar números amigables)
- Recta de Euler
- Seudo primos de Euler
- Sistema de Euler, una colección de clases de cohomología (UTF)
- Tipografía de Euler de la AMS
- Tira (spline) de Euler
- Trayectoria de Euler o ciclo de Euler (gráfica de los 7 puentes de Königsberg)

Teoremas:

- Teorema de Euclides–Euler
- Teorema de rotación de Euler
- Teorema de la función homogénea de Euler
- Teorema de Euler–Fermat:

$$a^{\varphi(m)} \equiv 1 (\text{mód} m)$$

  siempre que a sea primo relativo a m, φ es la función fi de Euler
- Fórmula de Euler–Maclaurin, un teorema acerca de integrales
- Teorema de Euler en geometría, relaciona los radios del círculo circunscrito y el círculo inscrito de un triángulo.

Tomado principalmente de: http://en.wikipedia.org/wiki/Leonhard_euler (Wikipedia)

7. Comentarios

Algunos amables, otros un tanto amargos

Refiriéndose al nacimiento de la teoría de números moderna **André Weil** dice que ésta ha de haber nacido dos veces ubicando el primero en algún punto entre 1621 (cuando Bachet publicó su aritmética de Diofanto) y 1636 (se sabe por su correspondencia que para entonces Fermat ya la había estudiado cuidadosamente y desarrollaba ideas propias acerca de varios temas considerados en ella).

A partir de entonces la teoría de números nunca dejó de estar entre los mayores intereses de Fermat; pero sus valientes esfuerzos para ganar adeptos para su tema favorito no fueron del todo coronados con el éxito. "No faltan mejores temas en los cuales ocupar nuestro tiempo" fue el comentario de **Huygens** a Wallis.

El segundo nacimiento de la teoría de números lo ubica Weil el 4 de junio de 1730 cuando Euler, motivado por preguntas de su amigo Goldbach, expresa "justo he estado leyendo a Fermat" y que está muy impresionado por su afirmación de que todo entero es suma de cuatro cuadrados.

Desde ese día Euler no se alejó de la teoría de números; eventualmente Lagrange continuó, después Legendre y más adelante Gauss con quien la teoría de números alcanzó total madurez. Aunque el tema nunca ha sido muy popular, se ha desarrollado bastante bien desde entonces.

En su prólogo al libro "Elementos de Álgebra" de Euler, **C. Truesdell** comenta que en una época en que el genio, la ambición intelectual y el ímpetu eran comunes, ninguno superaba a Euler en cualquiera, y ninguno se le acercaba en la combinación de los tres. No obstante, la historia del siglo XVIII y las historias sociales o intelectuales en general rara vez mencionan a Euler. La explicación fue escrita por **Fontenelle** (filósofo y científico francés, 1657–1757), antes del nacimiento de Euler:

"Tenemos gusto de considerar como inútil lo que no sabemos; es un tipo de venganza; y como las matemáticas y la física son algo generalmente desconocido, pasan generalmente por algo inútil. La fuente de su infortunio es simple; son espinosas, salvajes y difíciles de alcanzar .... Tal es el destino de las ciencias manejadas por pocos. La utilidad de su progreso es imperceptible para la mayoría de las personas, especialmente si practican profesiones no

particularmente ilustres.".

Nuevamente **Weil** nos comenta que **Poisson** expresó, en el discurso que dio en el funeral de Legendre, y que podría no haber tenido la aprobación de su difunto colega y maestro:

"Las cuestiones relativas a las propiedades de los números, aisladas de toda aplicación, tienen sólo un único atractivo, en verdad muy poderoso, sobre los matemáticos: la extrema dificultad que ellas presentan".

Contrasta esto con la propia declaración de **Legendre**, en el prefacio de su ensayo en teoría de números de 1798:

"Hay que creer ... que Euler tenía un gusto particular por esta clase de investigaciones, y que él las tomaba con una clase de pasión, como le sucede a casi cualquiera que se ocupa de ellas"

Seguramente, cuando escribía estas líneas, Legendre debe haber expresado su propio sentimiento acerca de lo que fue, junto con funciones elípticas, su tema favorito.

Francisco Larroyo cita a **Condorcet** refiriéndose a Euler:

"Cuando publicaba una memoria sobre un asunto nuevo, exponía con sencillez el camino que había recorrido, haciendo observar sus dificultades y vericuetos, y, luego de hacer seguir a sus lectores la marcha de su espíritu durante los primeros ensayos, les mostraba en seguida cómo había conseguido encontrar el camino más fácil demostrando así que prefería la instrucción de sus discípulos a la satisfacción que pudiera producirle el asombro de ellos, creyendo no hacer bastante por la ciencia si no agregaba, a las verdades nuevas con las que la enriquecía, la exposición de las ideas que lo condujeron a su descubrimiento."

Opina **Larroyo** más adelante:

"Euler es el más grande de los matemáticos suizos y uno de los mayores de todos los tiempos. Todas las ramas de la matemática se gratifican de su genio; y no sólo: en la propia filosofía de las matemáticas expone ideas tanto más meritorias cuanto que son concebidas por un espíritu creador, de una rara y pedagógica honestidad intelectual. En fin, su pensar representa una modalidad de filosofía matemática."

Referencias

[1] Euler, L., Elements of Algebra, Springer Verlag, 1972

[2] Larroyo, F., Filosofía de las Matemáticas, Editorial Porrúa, 1976

[3] Varadarajan, V.S., Euler Through Time: A New Look at Old Themes, AMS, 2006

[4] Weil, A., Number Theory, An approach through history from Hammurapi to Legendre, Birkhäuser, 1984

[5] http://en.wikipedia.org/wiki/Leonhard_euler (Wikipedia)

[6] http://www.leonhard-euler.ch/ (The Euler Commission)

[7] http://www.euler-2007.ch/en/euler.htm (EULER 2007)

[8] http://www.math.dartmouth.edu/ẽuler/tour/tour_00.html (THE EULER ARCHIVE)

[9] http://www.euler-2007.ch/doc/SIAM3910.pdf (CELEBRACIÓN 20 de abril)

[10] http://www.maa.org/euler_trip/Eitinerary.html (EN SAN PETERSBURGO)

[11] http://www.emis.de/projects/EULER/ (PORTAL)

[12] http://genealogy.math.ndsu.nodak.edu/html/id.phtml?id=38586 (Genealogy Project)

[13] http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/e.html#s19 (EL NÚMERO e)

[14] http://www.maa.org/reviews/EulerTime.html (RESEÑA LIBRO Varadarajan)

[15] http://scidiv.bcc.ctc.edu/Math/Euler.html (BIOGRAFÍA BCC)

[16] http://www-gap.dcs.st-and.ac.uk/~history/Biographies/Euler.html (BIOGRAFÍA GAP y UK)

[17] http://concise.britannica.com/ebc/article-9033216/Leonhard-Euler (BIOGRAFÍA)

[18] http://www.maa.org/news/howeulerdidit.html

[19] http://www.physics.ucla.edu/class/85HC_Gruner/bios/euler.html (BIOGRAFÍA ucla)

[20] http://www-groups.dcs.st-and.ac.uk/~history/Extras/Euler_Fuss_Eulogy.html (FUSS)

8. Celebraciones

Entre otras:

- Libro: The Genius of Euler: Reflections on his Life and Work, editado por William Dunham.
- Libro: Leonhard Euler por Emil A. Fellmann.
- Libro: Leonhard Euler: A Man to Be Reckoned with por Andreas K. Heyn y Alice K. Heyne (historieta).
- Homenaje en la iglesia de St. Martin en Basilea el 20 de abril de 2007.
- Evento en Basilea, San Petersburgo y Berlín del 1 al 14 de julio de 2007.
- Una búsqueda en Netscape dio 50 páginas de 10 entradas cada una.
- Este trabajo y su correspondiente presentación.

$$e^{i\pi} + 1 = 0$$

La Función ϕ de Euler

William D. Banks
Department of Mathematics
University of Missouri
Columbia MO 65211 USA
bbanks@math.missouri.edu

Florian Luca
Instituto de Matemáticas, UNAM
Ap. Postal 61-3 (Xangari), CP 58089
Morelia, Michoacán, México
fluca@matmor.unam.mx

V. Janitzio Mejía Huguet
Universidad Autónoma Metropolitana-Azcapotzalco
Departamento de Ciencias Básicas
Av. San Pablo No. 180,
Col. Reynosa Tamaulipas
Azcapotzalco
02200 México, D.F.
vjanitzio@gmail.com;
vjanitzio@yahoo.com.mx

Resumen

La función "phi de Euler" siempre ha ejercido fascinación entre quienes gustan de "La Teoría de los Números" y yo no he sido la excepción. Sin embargo, las conjeturas de Lehmer y Carmichael me motivaron a conocerla más de cerca.

Así que cuando fui invitado a platicar en "El Segundo Taller de Teoría de Números" en Xalapa, no dudé acerca del tema.

Los teoremas 6 y 7 ya se han podido probar sin hacer mención de los primos de Fermat, lo que introduce una sensible mejoría.

Ojalá sirva de motivación para que más personas se adentren en el hermoso universo que es "La Teoría de los Números".

Vaya mi agradecimiento para los organizadores del evento por las muchas atenciones que recibí durante mi estancia en esa hermosa ciudad que es Xalapa, Ver!

V. Janitzio Mejía Huguet

1. Historia

Los chinos sabían, en los años 500 A.C., que $p \mid 2^p - 2$ para cada número primo p.

En una carta de 1640 a Frenicle de Bessy, Fermat afirmó que tenía una prueba del hecho más general que para todo primo p y entero a,

$$(*) \qquad a^{p-1} \equiv 1 \pmod{p} \qquad \text{si } p \nmid a.$$

En 1676, Leibniz observó que, para todo entero n,

$$\begin{aligned} n^2 - n &\equiv n(n+1) \equiv 0 \pmod 2, \\ n^3 - n &\equiv n(n+1)(n+2) \equiv 0 \pmod 3, \end{aligned}$$

y de manera similar para 5 y para 7; pero que el resultado correspondiente no es cierto para 9 (por ejemplo con $n = 2$).

Euler fue el primero en publicar una prueba del teorema de Fermat, la presentó el 2 de agosto de 1736 [17] ante la Academia de St. Petersburgo. Utilizando el hecho de que $p \mid \binom{p}{k}$ para toda $1 \le k \le p-1$, encontró la relación

$$(n+1)^p - (n+1) \equiv n^p - n \pmod p,$$

lo que implica $(*)$ por inducción sobre n.

La *función de Euler* $\phi(\cdot)$, cuyo valor en el entero $a \ge 1$ se define por

$$\phi(a) := \#\{1 \le m \le a : \gcd(a,m) = 1\},$$

fué considerada por Euler en conexión con su generalización del teorema de Fermat. El siguiente resultado lo presenta Euler ante la Academia de St. Petersburgo el 15 de Octubre de 1759 [18]:

(Euler, 1759) Para cada entero $a \ge 1$,

$$(\star) \qquad \phi(a) = \prod_{p^\alpha \| a} p^{\alpha-1}(p-1).$$

(Euler, 1759) Para todos los enteros $a \ge 1$ y m tales que $\gcd(a,m) = 1$, se tiene que

$$a^{\phi(m)} \equiv 1 \pmod m.$$

Notación: Factorización canónica de $a \in \mathbb{N}$

$$a = 2^{\alpha} \prod_{i=1}^{s} p_i^{\alpha_i},$$

donde $\alpha \geq 0$, $s \geq 0$, p_i primos impares y α_i enteros positivos.

La notación $\phi(a)$ se debe a Gauss (1801); Euler usó la notación πa para $\phi(a)$, pero sólo a partir de su segunda prueba de $(\star)$ en 1780. Sylvester la llamó "totient function" en 1879.

2. Identidad Fundamental

(Gauss, 1801)

$$\sum_{d|n} \phi(d) = n, \quad \text{para todo } n \geq 1.$$

De

$$\sum_{d \neq 1, n} \phi(d) = (n-1) - \phi(n)$$

sigue que

Proposición 1. *n es primo si y sólo si $\phi(n) = n - 1$*

3. Las Notaciones de Landau y Vinogradov

Sean f y g funciones definidas en el conjunto de números naturales con g positiva. Decimos que $f = O(g)$, (Landau) si existe una constante $K > 0$ tal que

$$|f(x)| < Kg(x) \quad \text{para todo } x \geq 1.$$

Algunas veces usaremos

$$f \ll g \quad o \quad g \gg f, \text{ (Vinogradov)}$$

para decir que $f = O(g)$. Escribiremos

$$f \asymp g$$

si las dos $f \ll g$ y $g \ll f$ se cumplen.

Decimos que $f = o(g)$ si

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0.$$

En particular,

$$f(x) = o(1)$$

si y sólo si $f(x) \to 0$ cuando $x \to \infty$. Escribimos

$$f \sim g$$

si $f = (1 + o(1))g$.

4. Identidad de Abel

Teorema 1. *Para toda función aritmética $a(n)$, sean $A(x) = \sum_{n\le x} a(n)$ y f una función con derivada continua en $[1,\infty)$. Entonces tenemos*

$$\sum_{1\le n\le x} a(n)f(n) = A(x)f(x) - \int_1^x A(t)f'(t)dt.$$

Apliquemos la identidad de Abel a $a(n) = 1$, y $f(x) = \frac{1}{x}$, en este caso $A(x) = [x]$, $f'(x) = -\frac{1}{x^2}$.

$$\begin{aligned}\sum_{k=1}^{n} \frac{1}{k} &= \frac{A(n)}{n} + \int_1^n \frac{t - \{t\}}{t^2}dt \\ &= 1 + \log n - \int_1^\infty \frac{\{t\}}{t^2}dt + \int_n^\infty \frac{\{t\}}{t^2}dt.\end{aligned}$$

La última integral es $O(\frac{1}{n})$. Se sigue que:

$$\lim_{n\to\infty} \Big(\sum_{k=1}^{n} \frac{1}{k} - \log n\Big) = 1 - \int_1^\infty \frac{\{t\}}{t^2}dt.$$

Esta constante es la llamada *Constante de Euler-Mascheroni*, de la cual aún no sabemos si es o no un número racional:

$$\gamma = \lim_{n\to\infty} \Big(\sum_{k=1}^{n} \frac{1}{k} - \log n \Big).$$

$$\gamma = 0.57721566490153286\ldots$$

5. Promedios

Es claro que

$$\frac{1}{x} \sum_{n\le x} n = \frac{1}{2}\, x + O(1).$$

(Dirichlet, 1849 → Mertens, 1874 → Walfisz, 1963, [56])

$$\frac{1}{x} \sum_{n\le x} \phi(n) = \frac{3}{\pi^2}\, x + O\Big((\log x)^{2/3} (\log\log x)^{4/3} \Big).$$

Es claro que

$$\sum_{n\le x} \frac{1}{n} = \log x + \gamma + o(1),$$

donde γ es la constante de Euler.

(Landau, 1900, [30])

$$\sum_{n\le x} \frac{1}{\phi(n)} = \frac{315\zeta(3)}{2\pi^4} \left(\log x + C_0\right) + O\left(\frac{\log x}{x}\right),$$

donde

$$C_0 := \gamma - \sum_{p} \frac{\log p}{p^2 - p + 1}.$$

Sea $\pi(x) = \#\{p \le x : p \text{ primo}\}$.

El Teorema del Número Primo:

$$\pi(x) \sim \frac{x}{\log x}.$$

(Pillai, 1941, [44])

$$\frac{1}{\pi(x)} \sum_{p\le x} \phi(p-1) = C_1 x + O\left(\frac{x}{\log x}\right),$$

donde

$$C_1 = \frac{1}{2}\prod_{p\geq 2}\left(1 - \frac{1}{p(p-1)}\right)$$

es la constante de Artin.

6. La función ϕ es muy errática

De $\phi(p) = p - 1$ y $\frac{\phi(p)}{p} = 1 - \frac{1}{p}$ se siguen:

$$\limsup_{n\to\infty} \phi(n) = \infty, \qquad \limsup_{n\to\infty} \frac{\phi(n)}{n} = 1.$$

(Somayajulu, 1950, [54])

$$\limsup_{n\to\infty} \frac{\phi(n+1)}{\phi(n)} = \infty, \qquad \liminf_{n\to\infty} \frac{\phi(n+1)}{\phi(n)} = 0.$$

(Schinzel y Sierpiński, 1954, [49])
El conjunto de todos los números $\frac{\phi(n+1)}{\phi(n)}$, es denso en el conjunto de todos los reales positivos!
También es cierto que el conjunto de todos los números $\frac{\phi(n)}{n}$, es denso en el intervalo (0,1).

7. Cotas Inferiores

(Landau, 1903, [31])

$$\liminf_{n\to\infty} \frac{\phi(n)\log\log n}{n} = e^{-\gamma}.$$

En particular, $\phi(n) \gg \dfrac{n}{\log\log n}$.

Por otro lado...

(Nicolas, 1983, [41]) La desigualdad

$$\phi(n) < e^{-\gamma}\frac{n}{\log\log n}$$

se cumple para una infinidad de n.

8. Divisores

Para un entero positivo n escribimos $\tau(n)$ para el número de divisores de n.

La estimación

$$\frac{1}{x}\sum_{n\le x}\tau(n) = \log x + O(1)$$

se cumple.

¿Qué tal el promedio de la función $\tau(\phi(n))$? Como $\tau(m) \ge 2^{\omega(m)}$ y

$$\omega(\phi(n)) \ge (\tfrac{1}{2} + o(1))(\log\log n)^2$$

para casi todo n, tenemos obviamente

$$\frac{1}{x}\sum_{n\le x}\tau(\phi(n)) \ge 2^{(\frac{1}{2}+o(1))(\log\log x)^2}$$

(Luca-Pomerance, 2007, [38])
Existen dos constantes c_1, c_2 tal que

$$\frac{1}{x}\sum_{n\le x}\tau(\phi(n)) = \exp\left((c(x)+o(1))\sqrt{\frac{\log x}{\log\log x}}\right).$$

cuando $x \to \infty$ donde $c(x) \in [c_1, c_2]$. Se puede tomar

$$c_1 = e^{-\gamma/2}/7 \qquad \text{y} \qquad c_2 = 2^{3/2}e^{-\gamma/2}.$$

Para casi todo n, $\omega(n)$ y $\tau(n)$ dividen a $\phi(n)$.
¿Qué podemos decir del $\mathrm{mcd}(n, \phi(n))$?

(Erdös-Luca-Pomerance, 2007, [15])

(i)

$$\frac{1}{x}\sum_{n\le x}\mathrm{mcd}(n,\phi(n)) < x^{o(1)}.$$

(ii) Existe una constante $c > 0$ tal que

$$\frac{1}{x}\sum_{n\le x}\mathrm{mcd}(n,\phi(n)) \ge (\log x)^{c\log\log\log\log x}$$

se cumple para todo x grande.

9. Relaciones y Propiedades

9.1. Algunas relaciones

$$\sum_{n=1}^{\infty} \frac{\phi(n)}{n^s} = \frac{\zeta(1-s)}{\zeta(s)} \quad \textit{para } Re(s) > 2,$$

donde ζ es la función ζ de Riemann.

$$\sum_{n=1}^{\infty} \frac{\phi(n)q^n}{1-q^n} = \frac{q}{(1-q)^2}$$

$$\phi(n) \geq \sqrt{n}, \text{ para } n > 6$$

$$\phi(n) \leq n - \sqrt{n}$$

$$\frac{1}{\zeta(2)} \frac{n}{\sigma(n)} < \frac{\phi(n)}{n} < \frac{n}{\sigma(n)}, \quad n > 1$$

9.2. Algunas propiedades

La función ϕ es multiplicativa. Es decir que

(1) $$\phi(mn) = \phi(m)\phi(n) \text{ si } (m,n) = 1.$$

De

(*) $$\phi(a) = \prod_{p^\alpha \| a} p^{\alpha-1}(p-1).$$

se siguen: $\phi(a)$ es par para $a \geq 3$ y ϕ no es sobre $\mathbb{N}$!!

(2) $$\phi(a) = a \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

(3) $$\phi(a^n) = a^{n-1}\phi(a)$$

$$\phi(2^n) = 2^{n-1}$$

Escribiendo $a = 2^\alpha \prod_{i=1}^{s} p_i^{\alpha_i}$;

$$\phi(a) = 2^{\alpha-1} \prod_{i=1}^{s} p_i^{\alpha_i - 1}(p_i - 1) = 2^e b$$

Entonces $(\alpha - 1) + s \leq e$.

¿Cuándo $\phi(a)|a$?
Ya que a ha de ser par:

$$(\alpha-1)+s\le e\le\alpha,\quad (s-1)\le e-\alpha\le 0\ \Rightarrow s\in\{0,1\}$$

$$s=0\Rightarrow a=2^{\alpha}$$

$$s=1\Rightarrow a=2^{\alpha}p^{\beta}$$

$$\phi(a)=2^{\alpha-1}p^{\beta-1}(p-1)$$

sigue que $(p-1)|2p\ \Rightarrow (p-1)|2$, luego $p=3$. Por tanto

Teorema 2.

$$\phi(a)|a \text{ si y sólo si } a=2^{\alpha}3^{\beta},\ \text{con } \alpha>0 \text{ si } \beta>0.$$

10. Totients

Llamaremos a un entero $m\ge 1$ un *totient* si $m=\phi(n)$ para algún entero $n\ge 1$.

Los primeros totients son:

$$1,2,4,6,8,10,12,16,18,20,22,24,28,30,\ldots$$

Sea $\mathcal{F}$ el conjunto de todos los totients.

Como $\phi(p)=p-1$ para todo primo p, deducimos que $p-1\in\mathcal{F}$; por lo tanto,

$$V(x):=\#\{m\le x: m\in\mathcal{F}\}\ge\pi(x)\gg\frac{x}{\log x}.$$

¿Cual es el tamaño real de $V(x)$ cuando $x\to\infty$?

10.1. Aproximaciones para $V(x)$

(Pillai, 1929, [45]) $V(x)\ll\dfrac{x}{(\log x)^{(\log 2)/e}}$

(Erdős, 1935, [11]) $V(x)\ll_{\varepsilon}\dfrac{x}{(\log x)^{1-\epsilon}}$

(Erdős, 1945, [12]) $V(x)\gg\dfrac{x\log\log x}{\log x}$

(Erdős-Hall, 1973 y 1976, [13] y [14])

$$V(x)\ \gg\ \frac{x}{\log x}\exp\left(c_1(\log\log\log x)^2\right)$$

$$V(x)\ \ll\ \frac{x}{\log x}\exp\left(c_2(\log\log\log x)^{1/2}\right)$$

(Pomerance, 1986, [47])

$$V(x) \ll \frac{x}{\log x} \exp\left(c_3(\log\log\log x)^2\right)$$

(Maier-Pomerance, 1988, [39])

$$V(x) = \frac{x}{\log x} \exp\left((C + o(1))(\log\log\log x)^2\right)$$

11. Multiplicidades de Totients

Para cada totient $m \in \mathcal{F}$, sea

$$A(m) := \#\left(\phi^{-1}(m)\right) = \#\{n \geq 1 : \phi(n) = m\}.$$

De la cota inferior $\phi(n) \gg n/\log\log n$, resulta que $A(m) < \infty$.

Conjetura de Sierpiński: Para cada $k \geq 2$, existe $m \in \mathcal{F}$ con $A(m) = k$.

(Schinzel, 1961, [51]) La conjetura de Sierpiński es cierta bajo la Hipótesis H.

(Ford–Konyagin, 1997, [23]) La conjetura de Sierpiński es cierta para todo $k \geq 2$ par.

(Ford, 1999, [20]) La conjetura de Sierpiński es cierta.

12. Números de Mersenne y Fermat

De la expresión:

$$\frac{a^n - 1}{a - 1} = a^{n-1} + \ldots + 1$$

sigue que si $a^n - 1$ es primo, entonces $a = 2$.

Si $n = kl$;

$$\frac{a^n - 1}{a^l - 1} = a^{(k-1)l} + a^{(k-2)l} + \ldots + 1$$

entonces;

Teorema 3 (Cataldi-Fermat). *Si $2^n - 1$ es primo, n es primo.*

A los primos de la forma $2^p - 1$ para algún primo p, se les conoce como primos de Mersenne y se acostumbra denotarlos por M_p. Se ha conjeturado que existen una infinidad de Números de Mersenne $M_p = 2^p - 1$ que son primos. Se conocen 44.

12.1. Números Perfectos

Son aquellos que son iguales a la suma de sus divisores propios.

P	Decimal	Binario
P_1	6	110
P_2	28	11100
P_3	496	111110000
P_4	8128	1111111000000

Un número binario que consiste de n $1's$ es igual a

$$1 + 2 + 2^2 + \ldots + 2^{n-1} = 2^n - 1$$

Podemos conjeturar que los números perfectos son de la forma $2^{n-1}(2^n - 1)$.

Teorema 4 (Euclides-Euler). *Un número par es perfecto si y sólo si es de la forma*

$$2^{n-1}(2^n - 1), \text{ con } (2^n - 1) - \text{primo de Mersenne.}$$

12.2. Números de Fermat

Teorema 5. *Si $a^n + 1$ es primo, entonces a es par y $n = 2^n$.*

Demostración 1. *Si $n = kl$ con k impar*

$$\frac{a^n + 1}{a^l + 1} = a^{(k-1)l} - a^{(k-2)l} + \ldots + 1$$

Con $a = 2$, tenemos los números de Fermat

$$F_n = 2^{2^n} + 1.$$

$F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$.

Fermat conjeturó que todos los F_n eran primos, Sin embargo, el 26 de Septiembre de 1732, Euler presenta ante la Academia de St. Petersburg [19]:

$$641 | F_5.$$

Durante su larga vida académica, Euler regresó varias veces a este resultado y dió varias pruebas de la no primalidad de F_5.

Ahora se piensa que el número de primos de Fermat F_n es finito!

Sin embargo, los números de Fermat son primos relativos a pares.
De

$$F_{n-1}^2 = (2^{2^{n-1}} + 1)^2 = 2^{2^n} + 1 + 2 \cdot 2^{2^{n-1}}$$

se sigue

$$F_{n-1}^2 - 2(F_{n-1} - 1) = F_n$$

Luego

$$F_n - 1 = (F_{n-1} - 1)^2$$

$$F_n - 1 = (F_{n-2} - 1)^{2^2} = \ldots = (F_{n-k} - 1)^{2^k}.$$

Se sigue entonces que

$$(F_n,\ F_m) = 1.$$

En consecuencia, usando únicamente las propiedades aritméticas de los números de Fermat, podemos concluir:

Existen una infinidad de números primos!

13. No totients

Investigando acerca de números no-totients, obtuvimos los siguientes resultados: Suponiendo que $2^e b$, b–impar es un totient:

$$2^k b = \phi(a) = \prod_{i=1}^{s} p_i^{(\alpha_i - 1)}(p_i - 1)$$

luego $p_i - 1 = 2^k c_i,\ \alpha_i \leq e,\ c_i | b\ i = 1 \ldots s$. Lo que prueba la siguiente

Proposición 2. *Si los números $2^\alpha c + 1$ son compuestos, para $\alpha \leq k$, y todo divisor $c|b$, entonces $2^k b$ no es un totient.*

En el caso en que $b = p - primo$, podemos decir más:
Si $2^e p = \phi(a) = 2^{\alpha-1} \prod_{i=1}^{s} p_i^{\alpha_i - 1}(p_i - 1)$

$$2^{(e+1-\alpha)} p = \prod_{i=1}^{s} p_i^{\alpha_i - 1}(p_i - 1).$$

Caso 1) Si $p = p_1$, entonces

$$2^{(e+1-\alpha)} p = p^{(\alpha_1 - 1)}(p - 1) \prod_{i=2}^{s} p_i^{\alpha_i - 1}(p_i - 1)$$

$\alpha_1 = 2\ y\ p - 1 | 2^{e+1-\alpha},\ \alpha_i = 1,\ i = 2 \ldots s,\ p - 1 = 2^k$ (primo de Fermat), $k \leq (e + 1 - \alpha)$. Luego $a = 2^\alpha p^2 \prod_{i=2}^{s} p_i$, p, p_i primos de Fermat. Claramente, podemos tomar a de la forma

$$a = 2^{\alpha+m} p^2.$$

Caso 2) Si $p | p_1 - 1$, se sigue que $p_1 - 1 = 2^k p\ \alpha_i = 1$

$$2^{e+1-\alpha} p = 2^k p \prod (p_i - 1).$$

Luego $a = (2^k p + 1) \prod p_i$, p_i primos de Fermat.

Así pues, hemos demostrado el siguiente

Teorema 6. *El número $2^e p$, p primo es un totient si y sólo si p es un primo de Fermat y $(p-1)|2^e$, o $2^k p + 1$ es primo para algún $k \leq e$.*

En consecuencia(o equivalentemente):

Teorema 7. *El número $2^e p$ no es un totient si y sólo si p no es un primo de Fermat o $(p-1)$ no es divisor de 2^e y $2^k p + 1$ es compuesto para $k \leq e$.*

Un par de corolarios:

Corolario 1. *El número $2p$, p primo es un totient si y sólo si $2p+1$ es un número primo (Primos de Sophie Germain).*

Corolario 2. *El número $4p$, p primo no es un totient si y sólo si $2p+1$ y $4p+1$ son números compuestos.*

Así, tenemos el siguiente conjunto de números no-totients:

{ 14, 26, 34, 38, 50, 62, 68, 74, 76, 86, 90, 94, 98, 114, 118, 122, 124, 134, 142, 146, 152, 154, 158, 170, 174, 182, 186, 188, 194, 202, 206, 214, 218, 230, 234, 236, 242, 244, 246, 248, 254, 258, 266, 274, 278, 284, 286, 290, 298, 302, 304, 308, 314, 318, ...}

14. Valores

n	$\phi(n)$	n	$\phi(n)$	n	$\phi(n)$	n	$\phi(n)$
1	1	21	12	41	40	61	60
2	1	22	10	42	12	62	30
3	2	23	22	43	42	63	36
4	2	24	8	44	20	64	32
5	4	25	20	45	24	65	48
6	2	26	12	46	22	66	20
7	6	27	18	47	46	67	66
8	4	28	12	48	16	68	32
9	6	29	28	49	42	69	44
10	4	30	8	50	20	70	24
11	10	31	30	51	32	71	70
12	4	32	16	52	24	72	24
13	12	33	20	53	52	73	72
14	6	34	16	54	18	74	36
15	8	35	24	55	40	75	40
16	8	36	12	56	24	76	36
17	16	37	36	57	36	77	60
18	6	38	18	58	28	78	24
19	18	39	24	59	58	79	78
20	8	40	16	60	16	80	32

15. Algunos Resultados

Existen una infinidad de enteros positivos k tales que $2^n k + 1$ es compuesto para cada $n \geq 0$. Tales k se llaman números de Sierpiński.

A los números k tales que $2^n k - 1$ es compuesto para cada $n \geq 0$ se les llama números de Riesel. También existen una infinidad de ellos, Erdös fué el primero en probar que hay una proporción positiva de ellos.

No se conocen aun los números más pequeños de Sierpiński o de Riesel.

En 1956, Schinzel [50] demostró que para todo $k \geq 1$, $2 \cdot 7^k$ no es un valor de la función ϕ.

En 1963, Selfridge y también Bateman dieron solución al problema propuesto por Ore [42]:

Para todo $e \geq 1$, existe un entero impar k_e tal que $2^e k_e$ no es un valor de la función ϕ.

En 1976, Mendelsohn [40] demostró que existen una infinidad de primos p tales que para todo $k \geq 1$, $2^k p$ no es un valor de la función ϕ de Euler.

Gupta [24] demostró en 1950, que:

- *Para cada n, hay un m tal que $\phi(m) = n!$*

Demostración: Escriba

$$n! = k \prod_{p \leq n} (p - 1).$$

Claramente,

$$k = \prod_{p \leq n} p^{\alpha_p}$$

para algunos $\alpha_p \geq 0$. Tomando

$$m = \prod_{p \leq n} p^{\alpha_p + 1}$$

nos da $\phi(m) = n!$.

¿Hay una infinidad de n tal que $\phi(n)$ es un cuadrado perfecto?

Respuesta: Si, $n = 2^{2k+1}$ para $k \geq 0$.

• *Hay una infinidad de n libres de cuadrados tal que $\phi(n)$ es un cuadrado.*

Demostración: Sea x grande. Toma $\mathcal{T} = \{p \leq x\}$. Para cada $\mathcal{S} \subset \mathcal{T}$ sea

$$n_{\mathcal{S}} = \prod_{p \in \mathcal{S}} p.$$

Hay $2^{\pi(x)}$ posibilidades para $n_{\mathcal{S}}$ y todos estos números son distintos por factorización única. Escriba

$$\phi(n_{\mathcal{S}}) = \prod_{p \in \mathcal{S}} (p-1) = d_{\mathcal{S}} u_{\mathcal{S}}^2,$$

donde $d_{\mathcal{S}}$ es libre de cuadrados. Como $P(d_{\mathcal{S}}) \leq x/2$ (aqui $P(n)$ es el máximo divisor primo de n y $P(1) = 1$), obtenemos que hay sólo $2^{\pi(x/2)}$ valores para d. Por el principio de las casillas hay un $\mathcal{A} \subset \mathcal{T}$ tal que

$$d_{\mathcal{A}} = d_{\mathcal{B}}$$

se cumple con $2^{\pi(x)-\pi(x/2)}$ subconjuntos $\mathcal{B}$ de $\mathcal{T}$. Queda notar que al tomar $n_{\mathcal{A}\Delta\mathcal{B}}$ sobre tales $\mathcal{B}$, todos los enteros obtenidos de esta manera son libres de cuadrados, distintos por factorización única (porque los subconjuntos de $\mathcal{T}$ con la operación Δ forman un grupo), y sus funciones de Euler son cuadrados.

16. La Conjetura de Carmichael

Conjetura: Sea $n \in \mathbb{N}$. Si la ecuación $\phi(x) = n$ tiene solución, entonces tiene al menos dos soluciones.

Dickson [8], p. 137 nos dice que en 1907 Carmichael [4] creyó probar este resultado y que desarrolló un método para encontrarla [5]. El resultado aparece como un ejercicio en Carmichael [6]. Sin embargo, Carmichael [7] descubrió un error en su demostración y desde entonces la conjetura permanece abierta.

Cualquier contraejemplo a la conjetura debe tener más de 10^7 dígitos [48].

Ford, [21] y [22], demostró que si existe un contraejemplo a la Conjetura de Carmichael, entonces una proporción positiva de totients son contrajemplos.

Existen ejemplos de números pares n para los cuales no existe un número impar m tal que $\phi(m) = \phi(n)$. Lorraine Foster [25] encontró $n = 33817088 = 2^9 \cdot 257^2$ como el menor de ellos.

17. Función Lambda de Carmichael

Definición:

$$\lambda(1) = 1 = \phi(1),$$
$$\lambda(2) = 1 = \phi(2),$$
$$\lambda(4) = 2 = \phi(4),$$
$$\lambda(2^k) = 2^{k-2} = \frac{1}{2}\phi(2^k) \text{ para } k \geq 3,$$
$$\lambda(p^k) = (p-1)p^{k-1} = \phi(p^k), \ p \text{ primo impar y } k \geq 1,$$
$$\lambda(p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}) = mcm(\lambda(p_1^{k_1}), \lambda(p_2^{k_2}), \ldots, \lambda(p_r^{k_r})),$$

donde $p_1, p_2, \ldots, p_r$ son primos distintos y $k_i \geq 1$ para $1 \leq k \leq r$.

Entonces

$$\lambda(n)|\phi(n) \text{ para todo } n \text{ y}$$

$\lambda(n) = \phi(n)$ si y sólo si $n \in \{1, 2, 4, q^k, 2q^k\}$, donde q es un primo impar y $k \geq 1$.

Nota: $\lambda(n)$ puede ser mucho más pequeño que $\phi(n)$ si n tiene muchos factores:

$$Sea\ n = 2^6 \cdot 11 \cdot 17 \cdot 41 = 490688, \ entonces$$
$$\lambda(n) = mcm(\lambda(2^6), \lambda(11), \lambda(17), \lambda(40))$$
$$= mcm(16, 10, 16, 40) = 80$$
$$\phi(n) = \phi(2^6)\phi(11)\phi(17)\phi(41) = 204800$$

El siguiente teorema generaliza el teorema de Euler y prueba que $\lambda(n)$ es un orden (exponente universal):

Teorema 8 (Carmichael). *Sean $a, n \in \mathbb{N}$. Entonces*

$$a^{\lambda(n)} \equiv 1 \pmod{n}$$

si y sólo si $(a, n) = 1$. Además, existe un entero b tal que

$$\mathrm{ord}_n b = \lambda(n).$$

Ya que $\phi(n) = \#\{\mathbb{Z}_n^*\}$, la cardinalidad del grupo de unidades de $\mathbb{Z}_n$, se desprende de las observaciones anteriores que éste es un grupo cíclico si y sólo si $n \in \{1, 2, 4, q^k, 2q^k\}$.

18. Pseudoprimos

Recíproco al teorema de Fermat

Si $a^{n-1} \equiv 1 \pmod{n}$, entonces n es primo.

Los antiguos chinos pensaban que si $2^n \equiv 2 \pmod{n}$, entonces n debe ser primo. Lo cual es cierto hasta $n \leq 340$. Sarrus 1819, es falso para $n = 341 = 11 \cdot 31$.

Definición 1. *Un número compuesto es llamado pseudoprimo si* $2^n \equiv 1 \pmod{n}$.

Teorema 9. *Si n es un pseudoprimo impar, entonces también lo es $N = 2^n - 1$.*

19. Números de Carmichael

En 1907 Robert D. Carmichael estableció la existencia de números compuestos n tales que $a^{n-1} \equiv 1 \pmod{n}$ para todos los enteros positivos a primos relativos a n. Los primeros números de Carmichael son:
{561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, ...}

Teorema 10 (Alford, Granville, Pomerance, 1994, [1]). *Los números de Carmichael son infinitos.*

Teorema 11. *Las siguientes proposiciones son equivalentes:*

1. *n es de Carmichael.*
2. $\lambda(n) | n - 1$
3. *n es libre de cuadrados y si $p|n$, entonces $p - 1 | n - 1$. De hecho $p - 1 | \frac{n}{p} - 1$. (Criterio de Korselt)*

Es fácil ver que n debe de ser impar y que tiene al menos tres factores primos.

20. La Conjetura de Lehmer

Conjetura de Lehmer: Si n es compuesto, entonces $\phi(n) \nmid n - 1$.

En 1932, Lehmer [32] demostró que un tal n debe de ser impar y libre de cuadrado y que el número de divisores distintos $\omega(n)$ debe cumplir $\omega(n) \geq 7$. Posteriormente se extendió a $\omega(n) \geq 11$. El mejor resultado conocido es $n \geq 10^{22}$ y $\omega(n) \geq 14$. Se conocen mejores resultados en casos particulares. Es evidente que si n satisface la conjetura de Lehmer, entonces n es un número de Carmichael.

21. Resultados

Sea

$$L(x) := \#\{n \leq x : n \text{ compuesto y } \phi(n) \mid n-1\}.$$

(Pomerance, 1977, [46])

$$L(x) \ll x^{1/2}(\log x)^{3/4}(\log\log x)^{-1/2}$$

(Shan, 1985, [52])

$$L(x) \ll x^{1/2}(\log x)^{1/2}(\log\log x)^{-1/2}$$

(Banks-Luca, 2006, [2])

$$L(x) \ll x^{1/2}(\log\log x)^{1/2}$$

(Křížek–Luca, 2001, [29])
Si $\phi(n)^2 \mid n^2 - 1$ entonces $n \in \{1, 2, 3\}$.
Definición: Decimos que un número n tiene la propiedad de Lehmer si es compuesto y $\phi(n)|n-1$.
(Deaconescu, 2006, [9])
Deaconescu estudia números con la propiedad de Lehmer y alguna estructura adicional y concluye que han de ser un número finito.
Por ejemplo, el demuestra que si $k \geq 1$ fijo entonces existen un número finito de enteros positivos con la propiedad de Lehmer que satisfacen la congruencia

$$\phi(n)^k \equiv 1 \pmod{n}.$$

En relación con la sucesión de Fibonacci $\{F_n\}_{n\geq 0}$ dada por $F_0 = 0$, $F_1 = 1$ y $F_{n+2} = F_{n+1} + F_n$ para $n \geq 0$, se tiene:
(Luca, 2007, [36])
No existen números de Fibonacci con la propiedad de Lehmer.

22. Algunos Problemas Abiertos

- ¿Se cumple $\phi(n) = \phi(n+1)$ para una infinidad de n?
- ¿Son $\phi(n)$ y $\phi(n+1)$ simultaneamente cuadrados perfectos para una infinidad de n?
- (Totients-gemelos) Es $m+2 \in \mathcal{F}$ para una infinidad de $m \in \mathcal{F}$?
- (Erdös) Existen una infinidad de parejas de enteros (m, n) tales que $\phi(m) = \sigma(n)$.

23. Miscelánea

23.1. Curiosidades Numéricas, Ejemplos ...

$$\begin{aligned}
\phi(1) &= 1 \\
\phi(21) &= 12 \\
\phi(63) &= 36 \\
\phi(270) &= 72 \\
\phi(291) &= 192 \\
\phi(2991) &= 1992 \\
\phi(6102) &= 2016
\end{aligned}$$

23.2. Diversión con el Teorema de Euler

El Teorema de Euler:

$$n \mid a^{\phi(n)} - 1 \quad \text{si} \quad \gcd(a, n) = 1.$$

Menos conocido pero también cierto:

$$n \mid \phi(a^n - 1) \quad \text{si} \quad a > 1.$$

Sea

$$\begin{aligned}
\mathcal{H}_a(x) &:= \{n \le x : \phi(n) \mid a^n - 1\}, \\
\mathcal{G}_a(x) &:= \{n \le x : n \mid \phi(n)^a - 1\}.
\end{aligned}$$

(Banks-Luca-Shparlinski, 2005, [3])

$$\#\mathcal{H}_a(x) \le \frac{x}{\exp\left(\left(2^{-1/2} + o(1)\right)\sqrt{\log x \log\log\log x}\right)}$$

Si a es par, entonces

$$\begin{aligned}
\#\mathcal{G}_a(x) - \pi(x) & \\
&\ll \frac{x}{\exp\left(\left(2^{-1/2} + o(1)\right)\sqrt{\log x \log\log x}\right)},
\end{aligned}$$

y si a es impar, entonces

$$\#\mathcal{G}_a(x) \le \frac{x}{\exp\left(\left(2^{-1/2} + o(1)\right)\sqrt{\log x \log\log x}\right)}.$$

23.3. $\phi(n)$ Libre de Cuadrados

La relación de Euler:

$$\phi(n) = \prod_{p^\alpha \| n} p^{\alpha-1}(p-1),$$

Si $m = \phi(n)$ es *libre de cuadrados*, entonces:

- Si p divide a n, entonces $p-1$ es libre de cuadrados;
- $p^3 \nmid n$ para ningún primo p;
- Si $4 \mid n$, entonces $p \nmid n$ para ningún otro $p \neq 3$, por lo tanto, $n = 4$;
- Si $4 \nmid n$, entonces $p \mid n$ para a lo más un $p \neq 2$.

Por lo tanto, $n \in \{2, 4, p, 2p, p^2, 2p^2\}$ para algún $p \neq 2$ tal que $p-1$ es libre de cuadrados.

Sean

$$\begin{aligned} \mathcal{P}_2(x) &:= \{p \leq x : p-1 \text{ es libre de cuadrados}\}, \\ \mathcal{A}_2(x) &:= \{n \leq x : \phi(n) \text{ es libre de cuadrados}\}. \end{aligned}$$

(Pappalardi-Saidak-Shparlinski, 2003, [43])

Para cada constante $K > 0$,

$$\#\mathcal{P}_2(x) = \alpha_2\, \pi(x) + O\left(\frac{x}{(\log x)^K}\right),$$

donde α_2 es la constante de Artin.

Para cada constante $K > 0$, se tiene que

$$\#\mathcal{A}_2(x) = \frac{3\alpha_2}{2}\, \pi(x) + O\left(\frac{x}{(\log x)^K}\right).$$

23.4. Curiosidades Numéricas, Resultados

(Luca, 2005, [35]) Si $b > 1$ es fijo, entonces

$$\phi(\underbrace{\overline{a \ldots a}}_{n \text{ veces}}) = \underbrace{\overline{cc \ldots c}}_{m \text{ veces}} \quad a,\ c \in \{1, \ldots, b-1\}$$

tiene sólo un número finito de soluciones en enteros a, c, m, n.

(Luca, 2000, [33]) Sea $\{F_n\}_{n \geq 0}$ la sucesión de Fibonacci. Entonces la solución más grande de

$$\phi(F_n) = 2^m$$

es $n = 7$.

(Luca-Mignotte, [37]) La solución más grande de

$$\phi(F_n) = \underbrace{\overline{dd \ldots d}}_{m \text{ veces}} \quad d \in \{1, \ldots, 9\},$$

es $n = 11$. $\phi(F_{11}) = 88$.

Referencias

[1] W. R. Alford, A. Granville, C. Pomerance, "There are infinitely many Carmichael numbers". Ann. of Math. (2) 139 (1994), no. 3, 703–722.

[2] W. D. Banks and F. Luca, "Composite Integers n for Which $\phi(n)|n-1$", to appear in Acta Mathematica Sinica, English Series, (2006).

[3] W. Banks, F. Luca and I. E. Shparlinski, "*Some divisibility properties of the Euler function, Glasgow Math. J.* **47** (2005), 517–528.

[4] R. D. Carmichael, "On *Euler's* φ-Funktion". Amer. M. S. Bull. (2) 13, (1907), 241-243.

[5] R. D. Carmichael, "Notes on the simplex theory of numbers". Amer. Math. Soc. Bull. (2) 15, 217-223. Published: (1909).

[6] R. D. Carmichael, "The Theory of Numbers". New York; Wiley, 1914.

[7] R. D.Carmichael, "Note on Euler's φ-function". (English) American M. S. Bull. 28, 109-110 (1922). Published: 1922.

[8] L. E. Dickson, "History of the Theory of Numbers", Vol. 1: Divisibility and Primality. New York; Dover, (2005).

[9] M. Deaconescu, "On The Equation $m-1=a\phi(m)$". Integers 6 (2006), A6, 6 pp.

[10] J. B. Dence and T. P. Dence, "Elements Of The Theory Of Numbers". Academic Press,(1999).

[11] P. Erdös, "On the normal number of prime factors of $p-1$ and some related problems concerning Euler's φ-function". Quart. Journ. of Math. 6, (1935), 205-213.

[12] P. Erdös, "Some remarks on Euler's ϕ-function and some related problems". Bull. Amer. Math. Soc. 51, (1945). 540–544.

[13] P. Erdös, R. R. Hall, "On the values of Euler's ϕ-function". Acta Arith. 22 (1973), 201–206.

[14] P. Erdös, R. R. Hall, "Distinct values of Euler's ϕ-function". Mathematika 23 (1976), no. 1, 1–3.

[15] P. Erdös, F. Luca, C. Pomerance, "On the proportion of integers coprime to an integer", to appear in the proceedings of the Conference "Anatomy of integer", Montreal, May 2006, Eds: J.-M. De Koninck, A. Granville and F. Luca, Published by the CRM, U. de Montréal, approx. 2008.

[16] P. Erdös, C. Pomerance, "On the normal number of prime factors of $\phi(n)$". Number Theory (Winnipeg, Man., (1983). Rocky Mountain J. Math. 15 (1985), no. 2, 343-352.

[17] L. Euler, "Theorematum quorandumad numeros primos spectantium demonstratio", Commentarii academiae scientiarum Petropolitanae 8, 1741, pp.141-146.

[18] L. Euler, "Theoremata arithmetica nova methodo demonstrata", Novi Commentarii academiae scientiarum Petropolitanae 8, 1763, pp 74-105.

[19] L. Euler, "Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus", Commentarii academiae scientiarum Petropolitanae 6, 1738, pp 103-107.

[20] K. Ford, "The number of solutions of $\phi(x) = m$", Ann. of Math. (2) 150 (1999), no. 1, 283–311.

[21] K. Ford, "The Distribution of Totients". Ramanujan J. **2**, 67-151, 1998.

[22] K. Ford, "The Distribution of Totients", *Electron. Res. Announc. Amer. Math. Soc.* **4**, 27-34, 1988.

[23] K. Ford, S. Konyagin, "On two conjectures of Sierpiński concerning the arithmetic functions σ and ϕ". Number theory in progress, Vol. 2 (Zakopane-Kościelisko, 1997), 795–803, de Gruyter, Berlin, 1999.

[24] H. Gupta, "On a problem of Erdös". Amer. Math. Monthly 57, (1950). 326–329.

[25] R. K. Guy, "Unsolved Problems in Number Theory".
Third Edition, Springer, (2004).

[26] G. H. Hardy and E. M. Wright,
"An Introduction To The Theory Of Numbers".
Fourth Edition, Oxford At The Clarendon Press.

[27] M. Krizek, F. Luca and L. Somer, "17 Lectures On Fermat Numbers".
CMS Books in Mathematics. Springer, (2001).

[28] T. Koshy, Elementary Number Theory with Applications.
Academic Press, (2002).

[29] M. Křížek and F. Luca: *On the congruence* $n^2 \equiv 1 \pmod{\phi(n)^2}$, *Proc. Amer. Math. Soc.* **129** (2001), 2191-2196.

[30] E. Landau, "Ueber die zahlentheoretische Function $\varphi(n)$ und ihre Beziehung zum Goldbach'schen Satz. Gtt. Nachr, (1900), 177-186.

[31] E. Landau, "Ueber den Verlauf der zahlentheoretischen Funktion $\varphi(x)$". Arch. der. Math. u. Phys. (3), 5, 86-91. Published (1903).

[32] D. H. Lehmer, "On Euler's totient function". (English) [J] Bulletin A. M. S. 38, 745-751.

[33] F. Luca, "Equations involving arithmetic functions of Fibonacci and Lucas numbers". Fibonacci Quart. 38 (2000), no. 1, 49–55.

[34] F. Luca, "Números Primos y Aplicaciones". Aportaciones Matemáticas, SMN, (2004).

[35] F. Luca, *On the Euler function of repdigits*, por aparecer en *Czechoslovak Math. J.*

[36] F. Luca, "Fibonacci numbers with the Lehmer property". Bull. Polish Acad. Sci. Math. 55 (2007), 7-15.

[37] F. Luca and M. Mignotte, $\phi(F_{11}) = 88$. Sometido.

[38] F. Luca, C. Pomerance, "On the average number of divisors of the Euler function". Publ. Math. Debrecen 70 (2007), no.1-2, 125-148.

[39] H. Maier, C. Pomerance, "On the number of distinct values of Euler's ϕ-function". Acta Arith. 49 (1988), no. 3, 263–275.

[40] N. S. Mendelsohn, "The equation $\phi(x) = k$". Math. Mag. 49 (1976), no. 1, 37–39.

[41] J.-L. Nicolas, "Petites valeurs de la fonction d'Euler". J. Number Theory 17 (1983), no. 3, 375-388. 11N37 (11A25)

[42] O. Ore, J. L. Selfridge, P. T. Bateman, "Advanced Problems and Solutions: Solutions: 4995". Amer. Math. Monthly 70 (1963), no. 1, 101–102.

[43] F. Pappalardi, F. Saidak and I. E. Shparlinski, "Square-free values of the Carmichael function". J. Number Theory 103 (2003), no. 1, 122–131.

[44] S. S. Pillai, "On the sum function connected with primitive roots". Proc. Indian Acad. Sci., Sect. A. 13, (1941), 526-529.

[45] S.S. Pillai, "On some functions connected with $\varphi(n)$". (English) [J] Bulletin A. M. S. 35, (1929), 832-836.

[46] C. Pomerance, "On composite n for which $\varphi(n) \mid n-1$". II. Pacific J. Math. 69 (1977), no. 1, 177–186.

[47] C. Pomerance, "On the distribution of the values of Euler's function". Acta Arith. 47 (1986), no. 1, 63–70.

[48] A. Schlafly and S. Wagon, "Carmichael's Conjecture on the Euler Function is Valid Below $10^{10000000}$". Math Comput. **63**, 415-419, 1994.

[49] A. Schinzel, W. Sierpiński, "Sur quelques proprits des fonctions $\varphi(n)$ et $\sigma(n)$". Bull. Acad. Polon. Sci. Cl. III. 2 (1954), 463-466 (1955). 10.0X.

[50] A. Schinzel, "Sur l'quation $\phi(x) = m$". (French) Elem. Math. 11 (1956), 75–78.

[51] A. Schinzel, Remarks on the paper "Sur certaines hypothses concernant les nombres premiers". Acta Arith. 7 1961/1962 1–8.

[52] Z. Shan, "On composite n for which $\varphi(n)|n-1$". J. China Univ. Sci. Tech. 15 (1985), no. 1, 109–112.

[53] D. Shanks, "Solved And Unsolved Problems In Number Theory". Fourth Edition, AMS Chelse Publishing, (2000).

[54] B. S. K. R. Somayajulu, "On Euler's totient function $\phi(n)$". Math Student 18, (1950), 31-32 (1951).

[55] I. Vinogradov, "Fundamentos de La Teoría de los Números". Segunda Edición, Editorial Mir, (1977).

[56] A.W. Walfisz, "Exponentialsummen in der neueren Zahlentheorie". Mathematische Forschungsberichte, XV. VEB Deutscher Verlag der Wissenschaften, Berlin, (1963), 231.

SEGUNDA PARTE

SECCIÓN

MAESTRÍA

Resolución de Problemas y uso de Tecnología en el Aprendizaje de Matemáticas

Fernando Barrera Mora
Universidad Autónoma del Estado de Hidalgo
Instituto de Ciencias Básicas e Ingeniería
Área Académica de Matemáticas
Ciudad Universitaria
Carretera Pachuca–Tulancingo Km 4.5
Colonia Carboneras
Mineral de la Reforma
42184 Pachuca, Hidalgo
barrera@uaeh.edu.mx

Resumen

En este artículo se discuten algunos aspectos relacionados con el uso de herramientas computacionales en el proceso de resolución de problemas. Particularmente, lo relacionado con la formulación de conjeturas cuando se han establecido con evidencias surgidas del uso de un sistema computacional. Se hace énfasis en la necesidad de presentar argumentos formales.

1. Introducción

Diversas investigaciones (Schoenfeld, 1992; NCTM, 2000) reportan aspectos relevantes del pensar matemáticamente cuando se compara el proceso del aprendizaje con el desarrollo de la disciplina. Entre estos se encuentra el proceso de formular y validar conjeturas. Este elemento del pensar matemáticamente adquiere otra dimensión, que debe ser explorada y entendida, cuando se incorporan herramientas tecnológicas en actividades de aprendizaje. En este contexto surgen preguntas naturales que pueden guiar la discusión. ¿Qué características deben incluir las actividades de aprendizaje para que el uso de herramientas tecnológicas permita identificar y ampliar los aspectos centrales del pensar matemáticamente? ¿Qué papel juegan las herramientas computacionales en el proceso de formular y validar conjeturas en los procesos del aprendizaje de las matemáticas? ¿Qué tan confiables son

los resultados matemáticos obtenidos con el uso de herramientas computacionales cuando se diseñan actividades de aprendizaje? La finalidad de este trabajo es mostrar algunos aspectos del pensar matemáticamente cuando se utiliza un sistema computacional para resolver problemas en geometría.

La discusión que haremos se enmarca en la *Resolución de Problemas*, marco referencial que establece una plataforma para examinar aspectos centrales en los procesos del aprendizaje de las matemáticas y su relación con la actividad propia del desarrollo de las matemáticas.

2. Aspectos del pensar matemáticamente

Cuando se trata de entender, desde un punto de vista sistemático, el problema en el aprendizaje de las matemáticas surgen de manera natural dos preguntas fundamentales. ¿Qué es aprender matemáticas? ¿Cuál es la naturaleza del pensar matemáticamente? Las respuestas posibles tendrán relación estrecha con la concepción que se tenga de las matemáticas. En este sentido dos concepciones opuestas emergen. Por un lado se considera que aprender matemáticas consiste en memorizar y aplicar una colección de reglas, principios, algoritmos, teoremas, definiciones y procedimientos para abordar ciertos problemas. Aunado a esto se considera que los problemas tienen una solución y una vez que se ha encontrado, la actividad termina. De esta concepción se desprende que la tarea de los estudiantes en el proceso de aprendizaje, consiste esencialmente en memorizar técnicas que les permitan abordar cierta clase de problemas, consecuentemente las matemáticas se consideran como algo terminado y estático.

En contraposición a este punto de vista y tomando como referencia los procesos que realizan los matemáticos profesionales, aprender matemáticas es antes que todo, desarrollar una actitud que valore los procesos del pensar matemáticamente. Al respecto Schoenfeld argumenta:

> Aprender a pensar matemáticamente significa (a) Desarrollar un punto de vista matemático que valore los procesos de matematización y abstracción y tener la tendencia de aplicarlos y (b) desarrollar competencias con las herramientas del oficio, y usarlas para lograr la meta de entender las estructuras y desarrollar el sentido matemático (Schoenfeld, 1994, pág. 60).

En los últimos 25 años, una corriente importante de la Educación Matemática ha centrado la atención en las características que presenta la *Resolución de Problemas*, desde el punto de vista del aprendizaje. El punto de partida es el trabajo de G. Polya (Polya, 1945), centrando la atención en la relación que existe entre los procesos que realizan los matemáticos profesionales al desarrollar la disciplina y los que desarrollan los estudiantes en las actividades de aprendizaje. Desde esta perspectiva Santos señala:

> Un principio fundamental, al considerar la resolución de problemas en el aprendizaje de las matemáticas, es aceptar que la actividad de aprender no se reduce a un conjunto de reglas que pueden aplicarse en la solución de problemas: es una perspectiva en la que existe una conceptualización dinámica de las matemáticas y en la cual es importante identificar elementos que ayuden a desarrollar y promover una disposición matemática en los estudiantes. (Santos, 2007, pág. 11).

De acuerdo con los argumentos mencionados, resulta de importancia considerar escenarios en los que se promuevan actividades de aprendizaje, así como un ambiente en donde la reflexión y comunicación de ideas matemáticas jueguen un papel central en los procesos.

Dado que la tecnología ha cambiado radicalmente la forma en que las ideas matemáticas se desarrollan, es natural preguntar: ¿qué elementos aporta el uso de herramientas tecnológicas al pensar matemáticamente? ¿Qué papel juega la tecnología en las demostraciones en matemáticas? ¿Cómo contribuye a desarrollar un punto de vista matemático el uso de sistemas computacionales en actividades de aprendizaje? ¿En qué medida cambia la concepción de las matemáticas en los estudiantes que se involucran en procesos de resolución de problemas mediados por tecnología? Con estas interrogantes en mente discutiremos algunos problemas que pudiesen ilustrar aspectos del pensar matemáticamente.

3. Problemas

Problema 3.1. *(Reyes Rodríguez, A. 2006) Dado un triángulo ABC y un punto P en el lado BC, ¿se puede construir un punto D en el lado AB de forma que área$(PBD) = \frac{1}{2}$área(ABC)?*

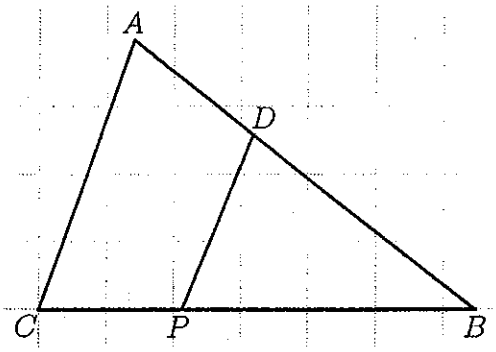


Figura 1: Dividir un triángulo en dos "partes iguales"

Discusión. Una primera pregunta para entender el problema pudiese ser. ¿Qué posición tiene el punto P? Si P es el punto medio del segmento BC, entonces eligiendo $D = A$ se resuelve el problema, pues los triángulos APB y APC tienen áreas iguales e iguales a la mitad del área del triángulo ABC. Si la posición de P es tal que la longitud del segmento PC es mayor que la longitud del segmento PB entonces no existe el punto D con la condición buscada, pues llamando M al punto medio del segmento BC y D cualquier punto del segmento AB se tiene que el triángulo PBD tiene área menor que la del triángulo MBA, que tiene área igual a la mitad de la del triángulo ABC.

Ahora examinaremos el caso en que el segmento PC tiene longitud menor que la del segmento PB. Haciendo uso de un sistema de geometría dinámica como Cabri Geometry, se observa que el área del triángulo PAB es mayor que el área del triángulo PAC, así que considerando un punto D *muy cerca* de A, el triángulo PDB todavía tiene área mayor que la del triángulo PAC, pero a medida que D se *aproxima* a B el área del triángulo PDB se *aproxima* a cero, pues también la altura se aproxima a cero. Mediante un argumento de *continuidad* o con la ayuda de Cabri Geometry se concluye que existe un punto D que satisface la condición requerida. ¿Cómo construirlo con regla y compás?

Trace la recta que contiene a B y C; sobre esta recta construya el punto B' de manera que P sea el punto medio del segmento BB'; trace el segmento AB' y por C trace la recta paralela al segmento AB', la cual interseca al segmento AB en un punto que llamaremos D. Demostraremos que este es

el punto buscado.

Por A y D tracemos perpendiculares al segmento BC, determinándose así los puntos S y T respectivamente. Ver la Figura 2. Por construcción, los triángulos $B'BA$ y CBD son semejantes, por lo que $\frac{B'B}{CB} = \frac{AB}{BD}$. Como $B'B = 2PB$, entonces

$$\frac{2PB}{CB} = \frac{AB}{BD}. \tag{1}$$

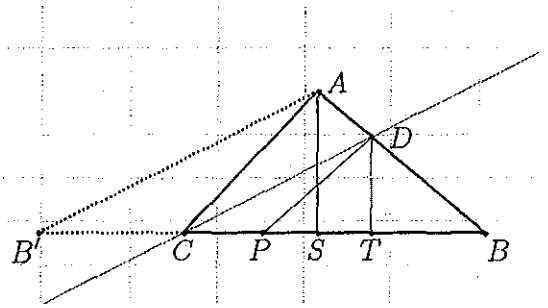


Figura 2: Construyendo el punto D

También se tiene que los triángulos ABS y BDT son semejantes, de esto se obtiene:

$$\frac{AB}{DB} = \frac{AS}{DT}. \tag{2}$$

Por otro lado, las áreas de los triángulos ABC y BDP están dadas por $\mathcal{A}(ABC) = \frac{1}{2}(BC)(AS)$ y $\mathcal{A}(BDP) = \frac{1}{2}(BP)(DT)$ respectivamente.

Sustituyendo en estas últimas ecuaciones los valores de BP y AS que se obtienen de (1) y (2) se tiene: $\mathcal{A}(ABC) = \frac{1}{2}(BC)\left(\frac{AB}{BD}\right)(DT)$ y $\mathcal{A}(BDP) = \frac{1}{4}\left(\frac{AB}{BD}\right)(BC)(DT)$. De esto último concluimos que $\mathcal{A}(BDP) = \frac{1}{2}\mathcal{A}(ABC)$, como se deseaba demostrar.

Una vez resuelto el problema planteado y dado que en algunos casos no hay solución surgen preguntas tales como: ¿bajo qué condiciones siempre existe D con las condiciones requeridas? ¿Para cuáles reales r se puede construir el punto D de forma que el triángulo PBD tenga área igual a r veces el área del triángulo ABC? Experimentando con Cabri Geometry se formula una conjetura cuya prueba da lugar al siguiente:

Teorema 3.1. *Dado un triángulo ABC y un punto P sobre la recta que contiene a uno de los lados, por ejemplo el lado BC, se puede construir con regla y compás un triángulo PDB tal que D esté en la recta que pasa por A y B, y $\mathcal{A}(DBP) = \frac{1}{2}\mathcal{A}(ABC)$.*

La demostración del teorema sigue las mismas líneas que en la discusión previa, salvo que ahora el punto D no necesariamente se encuentra en el segmento AB.

La segunda pregunta involucra a ciertos números reales y dado que en las construcciones euclidianas, las herramientas principales son la regla y el compás, centraremos la atención en los reales que se pueden construir con dichas herramientas. La respuesta se tiene en el siguiente:

Teorema 3.2. *Dado un triángulo ABC, r un real construible con regla y compás y un punto P sobre la recta que contiene a uno de los lados, digamos el lado BC, se puede construir con regla y compás un triángulo BDP tal que D esté en la recta que contiene al segmento AB, y $\mathcal{A}(BDP) = r\mathcal{A}(ABC)$.*

Antes de presentar la demostración del teorema, recordaremos como se construye, con regla y compás, el producto de dos números que a la vez son construibles con regla y compás.

Sean r y r' dos reales contruibles con regla y compás. En un sistema coordenado como se ilustra en la Figura 3, se traza una línea paralela a la línea que une a los puntos $(1,0)$ y $(0,r)$ y que pasa por $(r',0)$. Los triángulos formados por estas rectas y los ejes coordenados son semejantes. De esto se tiene que el punto de intersección de la recta que pasa por $(0,r')$ y el eje y es $(0,rr')$.

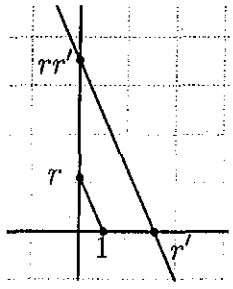


Figura 3: Dados r y r', se construye rr'

Demostración (del teorema). Sean L_1 y L_2 las líneas que contienen a los lados AB y BC respectivamente. Ver Figura 4. Sea B' en L_2 tal que

$$PB = rBB'. \tag{3}$$

Por el vértice C tracemos una paralela al segmento $B'A$ la cual interseca a la recta L_1 en el punto D; por los puntos A y D tracemos perpendiculares al segmento BC que lo intersequen en los puntos E y F respectivamente. Afirmamos que D es el punto que se busca.

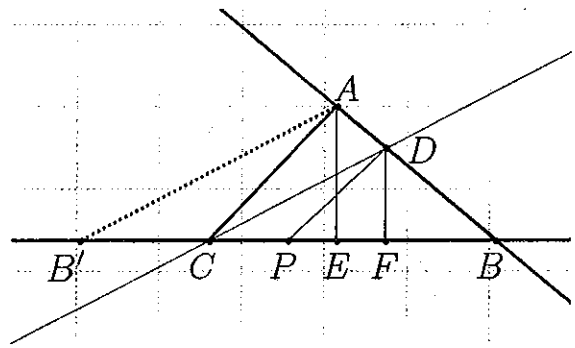


Figura 4: Construyendo el punto D

En efecto, se tiene:

$$\mathcal{A}(PBD) = \frac{1}{2}(PB)(DF) \tag{4}$$

$$\mathcal{A}(ABC) = \frac{1}{2}(BC)(AE). \tag{5}$$

De la construcción tenemos que los triángulos BCD y ABB' son semejantes, por lo que

$$\frac{BB'}{BC} = \frac{AB}{BD}. \tag{6}$$

Así mismo, los triángulos ABE y DBF también son semejantes, de lo cual obtenemos

$$\frac{BD}{DF} = \frac{AB}{AE}. \tag{7}$$

De las Ecuaciones 6 y 7 se tiene: $BD = \dfrac{(AB)(BC)}{(BB')} = \dfrac{(AB)(DF)}{(AE)}$, y de esta última obtenemos

$$(DF)(BB') = (AE)(BC). \tag{8}$$

De la Ecuación 3 se tiene que $(BB') = \frac{(PB)}{r}$, por lo que sustituyendo en (8) y usando (4) y (5) obtenemos la conslusión.

Una vez establecidos los resultados anteriores se puede preguntar. ¿Cuál es el lugar geométrico que describe el punto medio del segmento PD cuando P se mueve en la línea L_2? Ver Figura 5.

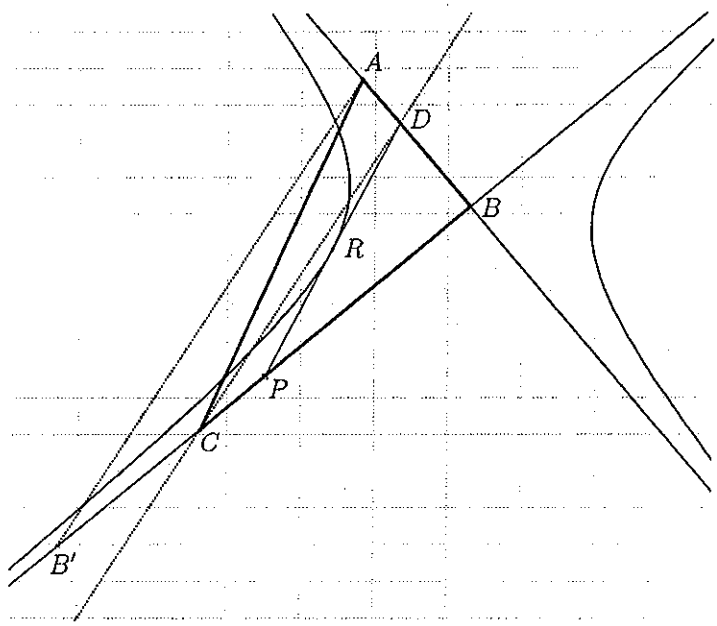


Figura 5: Lugar geométrico descrito por el punto medio de PD

Haciendo uso de la herramienta de Cabri Geometry, *lugar*, se muestra lo que aparece en la Figura 5. Aparentemente se trata de una hipérbola. En este momento, para un caso particular, podemos usar la herramienta de Cabri Geometry *Coord ó Ecuación* y preguntar qué ecuación tiene el lugar geométrico generado por R, obteniendo por respuesta $1.03x^2 - 1.07xy - 4.19y^2 + 6.03x + 8.28y - 10 = 0$. Con la información aportada por Cabri Geometry tenemos elementos para conjeturar que el lugar geométrico descrito por el punto medio de PD es una hipérbola, pues los coeficientes de los términos cuadráticos en x y y son de signo opuesto.

Usando un sistema coordenado

Sea R el punto medio de PD. Una posible forma de abordar la pregunta es hacer uso de un sistema coordenado y suponer que una de las rectas, por ejemplo L_2 coincide con el eje x. Ver Figura 6 después encontrar las coordenadas de R y determinar la relación que hay entre ellas.

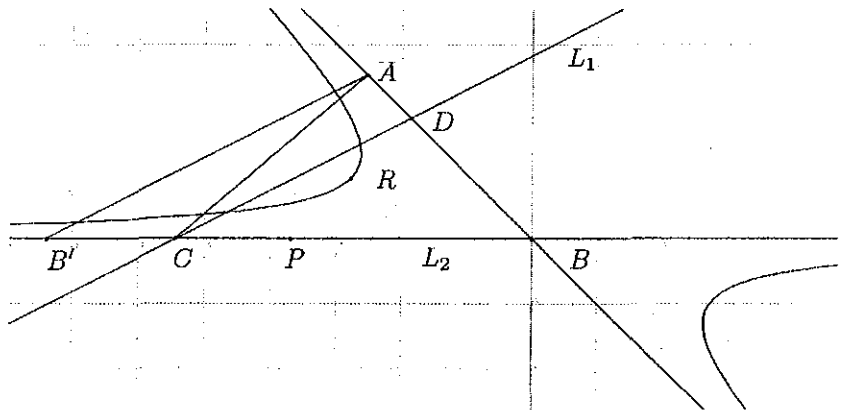


Figura 6: Usando coordenadas para describir el lugar geométrico generado por R

Podemos suponer que los vértices del triángulo y el punto B' tienen coordenadas: $A = (\alpha, \beta)$, $B = (0, 0)$, $C = (a, 0)$ y $B' = \left(\frac{m}{r}, 0\right)$ respectivamente, en donde $P = (m, 0)$ y r satisface $BB' = rPB$. La ecuación de L_1 está dada por:

$$y = \frac{\beta}{\alpha}x, \tag{9}$$

el segmento AB' tiene pendiente $m_1 = \dfrac{r\beta}{r\alpha - m}$. De esto concluimos que la recta que pasa por C y es paralela al segmento AB' tiene ecuación:

$$y = \frac{r\beta}{r\alpha - m}(x - a). \tag{10}$$

Resolviendo simultáneamente las Ecuaciones 9 y 10 se obtiene que las coordenadas del punto D son:

$$D = \left(\frac{ar\alpha}{m}, \frac{ar\beta}{m}\right), \tag{11}$$

por lo que las coordenadas de R satisfacen:

$$R = \frac{1}{2}\left(\frac{ar\alpha}{m} + m, \frac{ar\beta}{m}\right). \tag{12}$$

Llamando (x, y) a las coordenadas de R se obtiene $x = \frac{1}{2}\left(\frac{ar\alpha}{m} + m\right)$ y $y = \frac{ar\beta}{2m}$; eliminando el parámetro m en estas ecuaciones y simplificando concluimos que:

$$4\alpha y^2 - 4\beta xy + ar\beta^2 = 0. \tag{13}$$

Por otro lado, sabemos que la ecuación general $ax^2+bxy+cy^2+dx+ey+f = 0$ representa una hipérbola si $b^2-4ac > 0$. Aplicando este criterio a la Ecuación 13 se tiene que el lugar geométrico generado por R es una hipérbola, pues $16\beta^2 > 0$, ya que el punto $A = (\alpha, \beta)$ no está en el eje x.

Los resultados y discusión que se derivan del Problema 3.2, ilustran aspectos relacionados con el proceso de generalizar usando un sistema computacional y la necesidad de presentar pruebas al formular conjeturas "sustentadas" con datos generados por éste.

Problema 3.2. *Dada una recta L, $P \in L$ y $Q \notin L$, se traza el segmento PQ, la recta L_1 perpendicular a PQ en Q y la recta L_2 perpendicular a L en P. Sea $R \in L_1 \cap L_2$. ¿Qué lugar geométrico describe R al moverse P en L? Ver Figura 7.*

Una forma de aproximarse a la respuesta es efectuar la construcción con Cabri Geometry y hacer uso de la herramienta *lugar* con la cual se muestra que el lugar geométrico parece una parábola con vértice el punto Q. A partir de esto se puede intentar probar que en efecto, se trata de una parábola.

Iniciamos considerando un sistema coordenado y sin perder generalidad se puede suponer que la recta L coincide con el eje x. Adicionalmente, supongamos que el punto P tiene coordenadas $P = (t, 0)$ y el punto $Q = (a, b)$. Para determinar las coordenadas del punto R encontraremos las ecuaciones de las rectas L_1 y L_2 y resolveremos estas ecuaciones simultáneamente.

Como L_1 es perpendicular al segmento PQ y pasa por Q, para determinar su ecuación basta conocer la pendiente de tal segmento, la cual está dada por $m = \frac{b}{a-t}$, si $a \neq t$. Bajo esta condición se tiene que la ecuación de L_1 es $y - b = \frac{t-a}{b}(x-a)$ y la de L_2 es $x = t$. Resolviendo simultáneamente estas

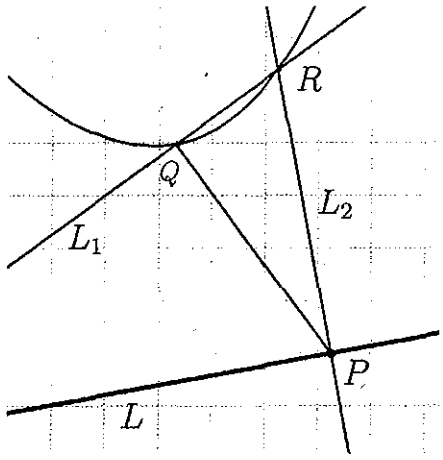


Figura 7: Lugar geométrico descrito por el punto R

ecuaciones se tiene que las coordenadas de R satisfacen $y - b = \dfrac{(x-a)^2}{b}$, pues $x = t$. Dado que a y b son fijos, en la ecuación anterior se identifica la ecuación de una parábola con vértice en (a, b) y longitud del lado recto igual a b. Como la distancia del foco al vértice es una cuarta parte de la longitud del lado recto, se tiene que el foco se localiza en $\left(a, \dfrac{5b}{4}\right)$ y la directriz está dada por $y = \dfrac{3b}{4}$, ver Figura 8.

Un aspecto interesante del problema anterior es que permite preguntarse por la forma en que Cabri Geometry efectúa ciertas transformaciones geométricas en el proceso dinámico. Para tal efecto, generalizamos el Problema 2 de la siguiente forma.

Sean L, P y Q como antes, tomamos un punto Q' en la línea que une a P y Q, efectuamos una construcción similar a la del problema anterior, salvo que ahora la línea perpendicular al segmento PQ pasa por Q'; ahora al mover P sobre L, el punto Q' también se mueve. Experimentando con Cabri Geometry se muestra que el lugar geométrico descrito por R parece ser una parábola; haciendo uso de la herramienta *Coord ó Ecuación* se verifica que la segunda coordenada del punto Q' no cambia al moverse P. Esto lleva a conjeturar que bajo esta hipótesis sobre Q', el lugar geométrico descrito por R es una parábola. De manera precisa:

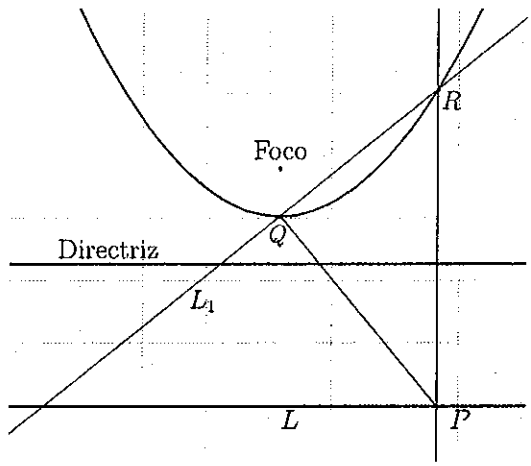


Figura 8: Lugar geométrico descrito por el punto R, ubicando foco y directriz

Teorema 3.3. *Consideremos un sistema cartesiano y L una recta que coincide con el eje x, ver Figura 9. Sean $P = (t, 0) \in L$, $Q = (a, b) \notin L$ y L_1 la recta que pasa por Q y P. Tomemos un punto $Q' = (c, d) \in L_1$. Supongamos que al mover P, la segunda coordenada de Q' no cambia. Sea L_2 la recta que pasa por Q' y es perpendicular a L_1. Designemos por R al punto de intersección de L_2 y la recta de ecuación $x = t$. Entonces el lugar geométrico descrito por R, al moverse P en L, es una parábola.*

Demostración Como se hizo antes, encontraremos las coordenadas del punto R y su relación.

Las rectas L_1 y L_2 tienen por ecuaciones:

$$y - b = \frac{b}{a - t}(x - a) \quad \text{y} \tag{14}$$

$$y - d = \frac{t - a}{b}(x - c), \tag{15}$$

respectivamente. La segunda coordenada de R se obtiene sustituyendo $x = t$

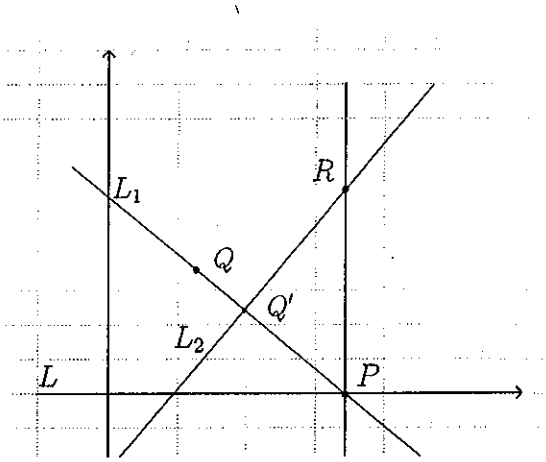


Figura 9: ¿Qué lugar geométrico describe R cuando se mueve P?

en la Ecuación 15, obteniéndose:

$$\begin{aligned} y-d &= \left(\frac{t-a}{b}\right)(t-c) \\ &= \left(\frac{t-a}{b}\right)(t-a-c+a) \\ &= \frac{(t-a)^2}{b}+\frac{a-c}{b}(t-a). \end{aligned} \tag{16}$$

Como $Q' \in L_1$, entonces:

$$d-b=\frac{b}{a-t}(c-a). \tag{17}$$

Despejando $a-c$ de (17) y sustituyendo en (16) se tiene:

$$\begin{aligned} y-d &= \frac{(t-a)^2}{b}+\frac{a-c}{b}(t-a) \\ &= \frac{(t-a)^2}{b}+\frac{d-b}{b^2}(t-a)^2 \\ &= (t-a)^2\left[\frac{1}{b}+\frac{d-b}{b^2}\right] \\ &= \frac{d}{b^2}(t-a)^2. \end{aligned} \tag{18}$$

Esta ecuación se puede escribir en forma equivalente:

$$\frac{b^2}{d}(y-d) = (t-a)^2 \tag{19}$$

que es la ecuación de una parábola con vértice en (a,d), foco en $\left(a, d+\frac{b^2}{4d}\right)$ y directriz de ecuación $y = d - \frac{b^2}{4d}$.

Una parte interesante del uso de Cabri Geometry para formular las conjeturas anteriores, es que al haber probado el teorema se obtiene información más precisa de la parábola. Por ejemplo, se conocen el foco y la directriz. Con ayuda de esto el teorema se puede formular en términos de geometría sintética.

Teorema 3.4. *Sean, L una recta, Q un punto fuera de L, $P \in L$, L_1 la recta que pasa por Q y P. Tome un punto $Q' \in L_1$ y trace la recta perpendicular a L_1 que pasa por Q', llamándole L_2. Por P, Q' y Q trace perpendiculares a L llamando a estas rectas L_3, L_4 y L_5 respectivamente. Sean T, S y R los puntos de intersección de las rectas L y L_4; L y L_5; L_2 y L_3 respectivamente. Por Q' trace una perpendicular a L_4 que interseque a L_3 y L_5 en E y V respectivamente. Sean F y W sobre L_5 tales que $WV = VF = \frac{QS^2}{4Q'T}$. Sea L_6 la perpendicular a L_5 que pasa por W e interseca a L_3 en U. Entonces L_6 y F son la directriz y foco de una parábola con vértice en V. Ver Figura 10*

Demostración.

La afirmación equivale a demostrar que $UR = FR$.

Aplicando el Teorema de Pitágoras y usando que $FA = VE$ tenemos:

$$FR^2 = VE^2 + (UR - 2VF)^2. \tag{20}$$

De los triángulos semejante $PQ'T$ y PQS se tiene:

$$\frac{QS}{Q'T} = \frac{VE}{Q'E}, \tag{21}$$

de lo cual obtenemos,

$$VE = \frac{SQ}{TQ'}Q'E. \tag{22}$$

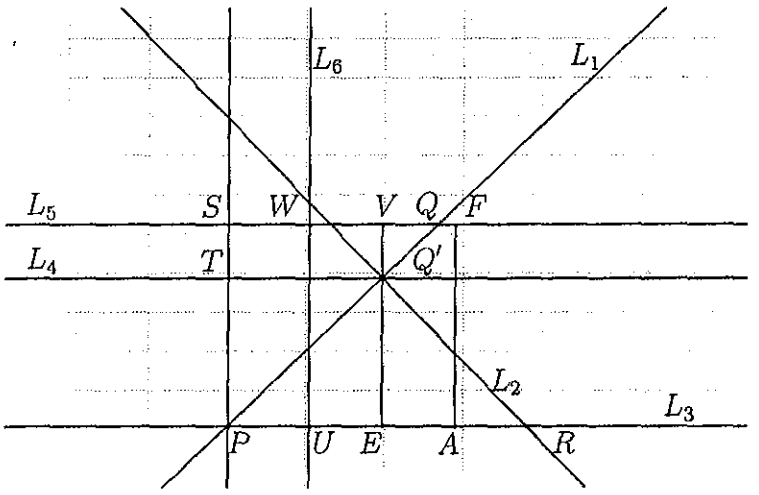


Figura 10: Se debe probar que $UR = FR$

Sustituyendo el valor de VF y VE en la Ecuación 20 y desarrollando el binomio se llega a:

$$\begin{aligned} FR^2 &= \frac{SQ^2Q'E^2}{Q'T^2} + UR^2 - UR\frac{QS^2}{Q'T} + \frac{QS^4}{4Q'T^2} \\ &= UR^2 + \frac{SQ^2}{Q'T}\left(\frac{Q'E^2}{Q'T} - UR + FV\right). \end{aligned}$$

Del triángulo rectángulo $RQ'P$ se tiene $Q'E^2 = (PE)(ER)$ y como $PE = Q'T$, entonces de la ecuación anterior se tiene

$$FR^2 = UR^2 + \frac{SQ^2}{Q'T}(ER - UR - FV). \tag{23}$$

Por otro lado $ER - UR = -EU = -VW = -VF$; de esto se concluye lo afirmado.

En el teorema anterior se tiene de hipótesis que la segunda coordenada del punto Q' no cambia; con esto en mente surge una pregunta natural. ¿Qué ocurre si esta hipótesis se cambia por: la distancia de Q a Q' no cambia? Con el uso de Cabri Geometry uno tiene la oportunidad de experimentar y observar el comportamiento del lugar geométrico generado por R. Una primera aproximación muestra resultados como se ilustra en la Figura 11,

y al parecer se trata de una parábola, incluso la herramienta de Cabri Geometry, *Ecuación*, propone como resultado que se trata de una parábola. Sin embargo, examinado más de cerca el comportamiento del lugar geométrico generado por R, aparece una gráfica como se muestra en la Figura 12, en la cual se muestra un objeto que no parece ser una parábola. Con estas evidencias es natural preguntar. ¿Es una parábola el lugar geométrico que describe R cuando se mueve P en L? Para precisar la respuesta, cambiando un poco la notación procedemos como sigue.

Dados, una recta L, un punto $P = (t, 0) \in L$, una circunferencia C de centro $O = (h, k) \notin L$ y radio r, se construyen las rectas L_1 que pasa por P y O; y L_3 que pasa por P y es perpendicular a L. Sean $Q \in L_1 \cap C$, L_2 la recta tangente a C que pasa por Q, R el punto de intersección de L_3 y L_2. ¿Es una parábola el lugar geométrico que describe R cuando se mueve P en L? Ver Figura 12

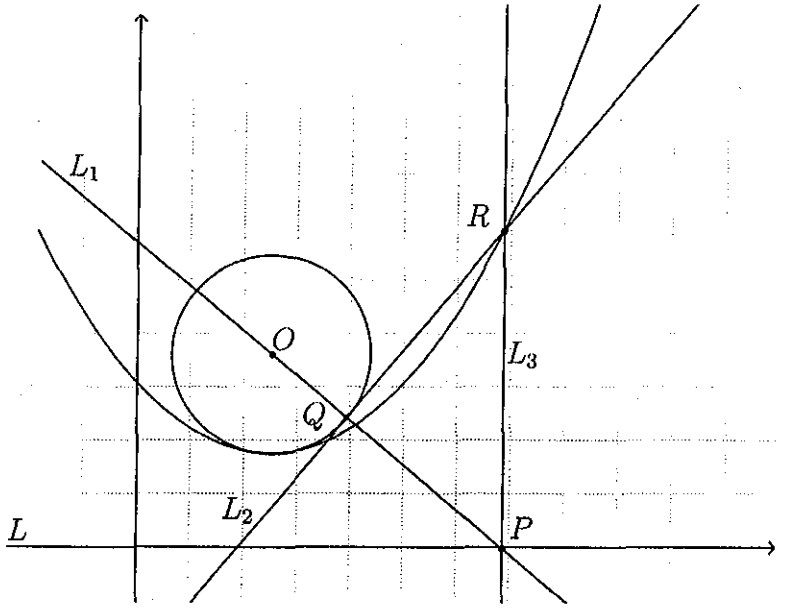


Figura 11: Lugar geométrico generado por R

Para determinar las coordenadas de R procedemos a encontrar las ecuaciones de L_1 y C, las cuales son:

$$y - k = \frac{k}{h - t}(x - h) \quad \text{y} \tag{24}$$

$$(x-h)^2+(y-k)^2=r^2, \tag{25}$$

respectivamente. Para determinar la ecuación de L_2, encontramos los puntos de intersección de C y L_1, resolviendo el sistema formado por las Ecuaciones 24 y 25.

Sustituyendo $y-k$ en la Ecuación 25 y resolviendo para x obtenemos:

$$x=h\pm\frac{r(h-t)}{\sqrt{(h-t)^2+k^2}}. \tag{26}$$

Sustituyendo este valor de x en (24) y simplificando se tiene:

$$y=k\left(1\pm\frac{r}{\sqrt{(h-t)^2+k^2}}\right). \tag{27}$$

Tomando los signos positivos en las ecuaciones anteriores se tiene que las coordenadas de Q son

$$Q=(x_0,y_0)=\left(h+\frac{r(h-t)}{\sqrt{(h-t)^2+k^2}},k\left(1+\frac{r}{\sqrt{(h-t)^2+k^2}}\right)\right). \tag{28}$$

Como L_2 es perpendicular a L_1, entonces la ecuación de L_2 es:

$$y-y_0=\frac{t-h}{k}(x-x_0). \tag{29}$$

De esto se tiene que la segunda coordenada de R se obtiene haciendo $x=t$ en la Ecuación 29, es decir, se tiene:

$$\begin{aligned} y &= \frac{t-h}{k}(x-x_0)+y_0 \\ &= \frac{t-h}{k}\left(t-h-\frac{r(h-t)}{\sqrt{(h-t)^2+k^2}}\right)+k\left(1+\frac{r}{\sqrt{(h-t)^2+k^2}}\right) \\ &= \left(\frac{(t-h)^2+k^2}{k}\right)\left(1+\frac{r}{\sqrt{(h-t)^2+k^2}}\right) \\ &= \frac{1}{k}\left((t-h)^2+k^2+r\sqrt{(t-h)^2+k^2}\right). \end{aligned}$$

Tomando los signos negativos en las expresiones para x y para y que se obtuvieron al resolver el sistema de ecuaciones (24) y (25) se tiene:

$$y=\frac{1}{k}\left((t-h)^2+k^2-r\sqrt{(t-h)^2+k^2}\right). \tag{30}$$

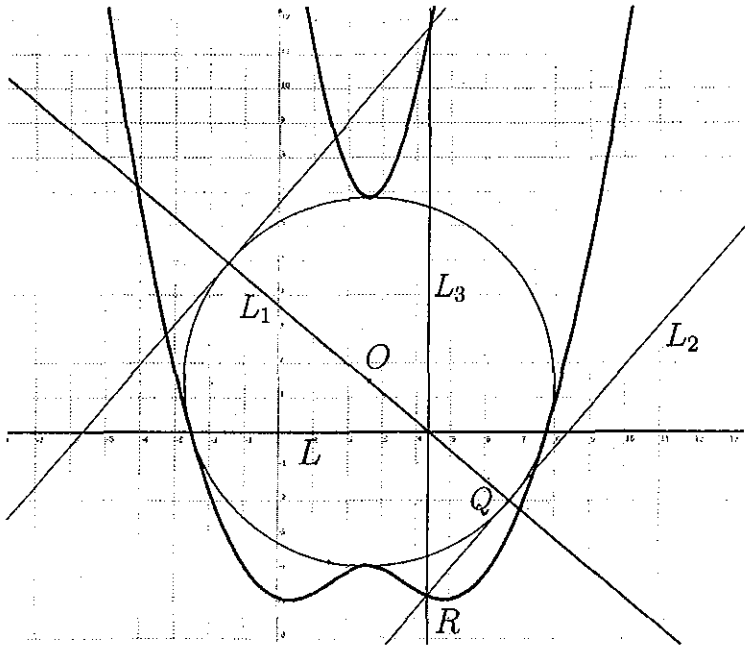


Figura 12: ¿Es una parábola el lugar geométrico generado por R?

De lo anterior se concluye que las coordenadas del punto R son

$$R = (t, \frac{1}{k}\left((t-h)^2 + k^2 \pm r\sqrt{(t-h)^2 + k^2}\right)) \tag{31}$$

y es claro que no satisfacen la ecuación de una parábola, sin embargo Cabri Geometry reporta que se trata de una parábola.

4. Conclusiones

En la introducción planteamos las siguientes interrogantes.

¿Qué características deben incluir las actividades de aprendizaje para que el uso de herramientas tecnológicas permita identificar y ampliar los aspectos centrales del pensar matemáticamente? ¿Qué papel juegan las herramientas computacionales en el proceso de formular y validar conjeturas en los procesos del aprendizaje de las matemáticas? ¿Qué tan confiables son

los resultados matemáticos obtenidos con el uso de herramientas computacionales cuando se diseñan actividades de aprendizaje?

Con los ejemplos discutidos hemos mostrado varios aspectos. Por un lado, las actividades de aprendizaje que se planteen debieran tener como finalidad que los estudiantes tengan la oportunidad de abordar su aprendizaje en un contexto de problematización, cuestionando sistemáticamente los resultados que se obtengan, así como experimentar y formular conjeturas. Esto debe ser fomentado como una práctica sistemática en los procesos de aprendizaje de los estudiantes.

Notamos que el uso de un sistema de geometría dinámica permite explorar y establecer conexiones entre diferentes contenidos, así como incorporar diferentes tipos de representaciones. Por ejemplo, la conclusión del Teorema 3.3 nos permitió, haciendo uso de un sistema coordenado, formular y demostrar el mismo teorema en términos de geometría sintética. Con esto se logra articular aspectos de la geometría analítica y la sintética y brinda la oportunidad de comparar las ventajas y desventajas al usar diferentes tipos de representaciones para abordar un problema.

Otro aspecto que es de crucial importancia al usar herramientas computacionales para resolver problemas matemáticos, es lo concerniente a los resultados que se obtienen, pues si bien un sistema computacional es una herramienta poderosa, los resultados que se obtengan deben ser sometidos a un examen riguroso y profundo, para aceptarlos o rechazarlos. Por ejemplo, el análisis en la última actividad muestra que los resultados de Cabri Geometry no concuerdan con el análisis algebraico realizado. Esto puede dar origen a una exploración a fondo del problema y preguntarse por la forma en que opera el software.

Referencias

[1] Kaput, J. (1992). Technology and mathematics education. In D. Grouws (Ed.),Handbook on research in mathematics teaching and learning, pp. 515–556. Mcmillan: New York.

[2] Polya, G. (1945). How to Solve it. Princeton University Press, Princeton USA.

[3] Reyes Rodríguez, A. (2006). Esquemas de razonamiento y prueba que utilizan profesores de bachillerato en la formulación y resolución de problemas en ambientes de geometría dinámica. Tesis de Maestría, Departamento de Matemática Educativa, CINVESTAV, México.

[4] Santos Trigo, M. (1999). The use of technology as a mean to explore mathematics qualities in proposed problems. In Fernando Hitt and Manuel Santos (Eds), Proceedings of the Twenty First Annual Meeting of the North American Chapter of the International Group for the Psycology of Mathematics Education, Vol I, Cuernavaca, México.

[5] Santos–Trigo, M. (2004). The role of [illegible] in the identification and construction of mathematical relationships. Journal of Computers in Mathematics and Science Teaching, 23 (4), pp, 399–413.

[6] [illegible]áticos. Fundamentos cognitivos. Edito[illegible] Trillas, México

[7] Santos–Trigo, M. & Barrera–Mora [illegible] (2007) Contrasting and looking into some mathematical [illegible]ication Frameworks. The Mathematics Educator, 10(1), pp. 81–106.

[8] NCTM (2000). Principles and Standards for School Mathematics, National Council of Teachers of Mathematics.

[9] Schoenfeld, A. (1994). "Reflections on doing and teaching mathematics", en A. Schoenfeld (ed) Mathematical thinking and problem solving, Hillsdale, Lawrence Erlbaum Associated Publishers, New Jersey, pp. 53–70.

[10] Schoenfeld, A. (2000). Porpuses and Methods of Research in Mathematics Education, Notices of the AMS, vol. 47, number 6.

Nociones de Teoría de Números en Arqueoastronomía, Calendarios y Ábacos Mesoamericanos

Alfonso Anzaldo Meneses
Universidad Autónoma Metropolitana–Azcapotzalco
Departamento de Ciencias Básicas
Av. San Pablo No. 180,
Col. Reynosa Tamaulipas
Azcapotzalco
02200 México, D.F.
alfons_rex@hotmail.com

Resumen

Resulta ser un lugar común el hablar someramente de las muy numerosas y a menudo asombrosas relaciones numéricas de los testimonios arquelógicos de Mesoamérica. Hay gran diversidad de interpretaciones que mas que facilitar la comprensión de los posibles conocimientos matemáticos subyacentes, las hacen incomprensibles. Al parecer, además de la complejidad del tema debida razones históricas, esto último se debe a que tales interpretaciones han sido hechas o bien por personas que no habitúan trabajar en Matemáticas o, en caso de ser así, que se han limitado a esbozar algunos aspectos particulares. En este trabajo presentamos una propuesta de análisis de las matemáticas mesoamericanas con fines didácticos que cumpla con el siguiente objetivo: Interesar al lector en el *estudio sistemático* de la teoría elemental de los números mediante procedimientos similares a aquellos que fueron necesarios para llevar a cabo tanto cálculos astronómicos como de otra índole en la antigüedad, por ejemplo para la elaboración de calendarios. Resaltamos la importancia que debió tener el ábaco de base veinte o NEPOHUALTZITZIN para la elaboración de todos los cálculos necesarios y damos una introducción a los algoritmos mas elementales para su uso.

1. Introducción

La comprensión del comportamiento de los astros requiere el estudio de los movimientos siguientes.

- **Movimiento de translación en el espacio**
- **Movimiento de rotación alrededor de su eje de simetría**
- **Movimiento de precesión de este eje**
- **Movimiento de nutación o cabeceo del eje sobrepuesto a la precesión**

La elaboración de **calendarios**, o para nosotros las **cuentas de los días**, tuvo por objetivo describir estos movimientos mediante cálculos numéricos por una parte y adicionalmente adecuar tal descripción a requerimientos sociales dados.

Supondremos que consideramos únicamente a los planetas que giran alrededor del sol y que éste se encuentra en reposo relativo (notemos no obstante que se mueve a 25 Km por segundo alrededor del centro de la galaxia).

La Tierra tiene aproximadamente el siguiente comportamiento. El movimiento de precesión terrestre era conocido posiblemente en el siglo II antes de nuestra cuenta (que abreviamos ac por las iniciales de *estas* palabras) en Grecia por el astrónomo Hyparcus, el cual daba la cifra de 46 segundos de arco por año, muy buen resultado en comparación con los 50.3 segundos medidos actualmente.

El ecuador de la tierra hace un ángulo de 23 grados y 27 minutos con la trayectoria alrededor del sol. Se denomina **eclíptica** a la trayectoria aparente del sol resultante de tal inclinación.

El movimiento rotacional terrestre lleva a la observación inmediata nocturna consistente en la rotación aparente de las estrellas alrededor de un punto llamado **polo de la bóveda celeste**. Si se divide al plano tangente a la tierra centrado en el punto de observación en las dos direcciones Norte–Sur y Este–Oeste, entonces el polo celeste se encuentra a una altura angular ϕ, que será igual a la latitud geográfica. En la actualidad la estrella *Alpha Ursae Minoris*, llamada **estrella polar** por razones obvias, se encuentra

a tan solo 0.9 grados del polo, pero debido al movimiento de precesión no siempre es la misma estrella la que se encuentra mas cerca del polo celeste. Entre los mayas la estrella polar se denominó *SAK XAMAN*, blanco–norte (ver *Fin y año nuevo mayas en los códices* de Hans Hasselkus, págs. 49, 96).

Notemos además que solamente aquellas estrellas que se encuentren a una distancia angular máxima $\phi_{\text{máx}}$. del polo celeste darán una órbita completa a su derredor. Las demás estrellas seguirán trayectorias semicirculares para desaparecer en algún momento en el horizonte celeste, su *ocaso*, y volver aparecer tiempo después por otro lado, su *amanecer*. Al punto más alto que alcanza una estrella en la bóveda celeste se le denomina como **culminación superior** y a su punto mas bajo como **culminación inferior**.

Una rotación terrestre **no** es igual a un *día solar medio* (ver definición mas abajo), sino que tiene una duración aproximada de 23 horas 56 minutos y 4 segundos. Lo cual se debe a la traslación de la tierra ya que durante el tiempo transcurrido entre las salidas del sol, la tierra se ha desplazado. La velocidad de rotación sobre la superficie de la Tierra en el ecuador es de aproximadamente 465.11 m/s (ó bien 1664 Km por hora) y decrece cosenoidalmente con la latitud ϕ, anulándose en los polos.

La inclinación de 23 grados y 27 minutos hace que en un punto del recorrido de la Tierra, el polo norte tenga una orientación máxima hacia el Sol, el punto del **solsticio de verano** del hemisferio norte. En otro punto opuesto al primero el polo sur se encuentra con una orientación máxima hacia el sol, el punto del **solsticio de invierno** del hemisferio norte. Finalmente hay dos puntos para los cuales tanto el polo norte como el polo sur tienen una orientación similar hacia el sol, estos son los puntos de los **equinoccios de primavera y de otoño**, respectivamente.

En el hemisferio norte la primavera dura aproximadamente 92 días y 22 horas, el verano 93 días y 14 horas, el otoño 89 días con 17 horas y el invierno 89 días y una hora, haciendo un total de 365 días con seis horas. La duración del tiempo que transcurre entre dos culminaciones solares consecutivas se denomina **día solar** y depende de la posición de la Tierra. En enero es más corto que en julio, ya que, como hemos recordado, el movimiento aparente del Sol es más rápido, respectivamente más lento, en dichos meses. Un reloj solar simple tendrá por ello temporadas en las que vaya adelantado y temporadas

en las que vaya atrasado.

Al tiempo que transcurre entre dos pasos aparentes del Sol por el punto de primavera se le conoce como **año trópico** y es el año que usualmente es considerado en la mayoría de los calendarios. **El año trópico tiene una duración actual aproximada de 365 días 5 horas 48 minutos y 45 segundos**, ó bien lo que es lo mismo de 365.242190 días. Los calendarios solares que aquí consideramos tuvieron como objetivo principal reproducir este número hasta la cuarta cifra decimal redondeada de una manera lo más simple posible satisfaciendo condiciones adicionales de índole diversa.

2. Los Calendarios de Sosígenes y de Clavius

El llamado *calendario juliano* fue decretado en Roma por Julio Cesar en el año 46 ac. Este calendario fue elaborado por el astrónomo alejandrino **Sosígenes**. Sosígenes elaboró un calendario solar basado en el año trópico con **duración promedio de 365.25 días**, esto es 365d6h, que estaba formado por tres años *normales* consecutivos de 365 días y de un año bisiesto de 366 días. Para mayor sencillez, todos los años divisibles por cuatro fueron seleccionados como bisiestos. La diferencia entre el año trópico y el año promedio del calendario Sosígenes, como lo llamaremos, era entonces de .007801 días, por lo que al cabo de 128.18869 años se acumulaba **un día de adelanto**. Este error se fue acumulando durante los siglos.

El matemático y astrónomo **Christopher Clavius** (1538-1612), nacido en Bamberg (ahora Alemania), fue encargado de corregir al calendario juliano en el siglo XVI, en colaboración con el astrónomo napolitano **Aloysius Lilius**, (1510-1576). Clavius propuso adoptar el calendario pagano vigente y hacer dos modificaciones muy simples.

1.) Definir como primer día del año al primero de enero previa adición de un número de días a la cuenta vigente. Esta modificación no es fundamental ni necesaria.

2.) **Todos los años de principios de siglo que no fuesen divisibles por cuatrocientos no fuesen bisiestos.**

Así pues, los años 1700, 1800 y 1900 no fueron años bisiestos, mientras que los años 1600 y 2000 si lo fueron. El calendario de Clavius tiene por tanto un período de 400 años que corresponden a 146097 días. Se obtiene como resultado **años de 365.2425 días**, o bien 365d5h49m12s, promediados

sobre 400 años. Los años de Clavius acumulan un **error de un día al cabo de aproximadamente 3322 años** y llevan desde 1582 hasta el 2002 un adelanto acumulado de poco más de 3 horas, esto es un octavo de día.

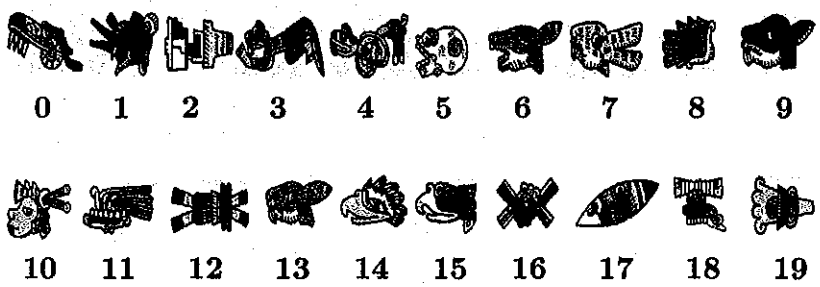
Una desventaja obvia de estos dos calendarios es que el primer día de la primavera, el equinoccio correspondiente, es en fechas que varían entre el 20 de marzo a las cero horas hasta el 21 de marzo al medio día, dependiendo de que se trate o no de años bisiestos. Por ejemplo, el inicio de la primavera el año 2004 fue el 20 de mayo a las 6h41m UT (longitud 0^o), esto es, al amanecer.

3. Los Calendarios de Anáhuac

Consideremos ahora someramente a los calendarios de la región de Anáhuac. Sobrevivieron pese al etnocidio diversas fuentes originales valiosísimas, como por ejemplo el Códice Dresden y el Códice Borgia. Se basan en un conjunto ordenado de **veinte símbolos** para los días y los años siguientes numerados del cero al diecinueve.

0. CIPACTLI. Cocodrilo.
1. EHECATL. Viento.
2. CALLI. Casa.
3. CUETZPALLIN. Iguana o lagartija.
4. COATL. Serpiente.
5. MIQUIZTLI. Muerte.
6. MAZATL. Venado.
7. TOCHTLI. Liebre o conejo.
8. ATL. Agua.
9. ITZCUINTLI. Perro.
10. OZOMATLI. Mono.
11. MALINALLI. Hierba.
12. ACATL. Carrizo.
13. OCELOTL. Ocelote o jaguar.
14. CUAUHTLI. Aguila.
15. COZCACUAUHTLI. Aguila de Collar.
16. OLLIN. Movimiento.
17. TECPATL. Pedernal.
18. QUIAHUITL. Lluvia.
19. XOCHITL. Flor.

Los glifos correspondientes son los siguientes.



Códice Borgia. Los días.

1. Ce **2.** **3.** Yei **4.** Nahui **5.** Macuilli (*de* maitl,*mano, y* cui *tomar*) **6.** Chicoace (*de* chico, *fracción*) **7.** Chicome **8.** Chicuey **9.** Chicnahui **10.** Matlactli (*de* maitl *mano, y de* tlactli, *busto, el cuerpo humano de la cintura para arriba*) **11.** Matlactli ihuan ce, *o bien* matlactli once **12.** Matlactli ihuan ome, *o bien* matlactli omome **13.** Matlactli ihuan yei, *o bien* matlactli omei

Además se formaron un conjunto de **18 veintenas** (esto es, 18 conjuntos de veinte días cada uno) y un conjunto llamado **NEMONTEMI** de aproximadamente cinco días. Usualmente corrían dos calendarios simultáneamente como veremos a continuación. El **XIUHPOHUALLI** es un calendario solar de los 360 días de las 18 veintenas mas los días NEMONTEMI (aquellos que dan por terminado un ciclo) haciendo un total de 365 días y fracción.

4. Nociones Útiles de Matemáticas

Es evidente que los **números naturales** denotados por medio del conjunto $\mathbb{N} = \{0, 1, 2, \dots\}$ son una herramienta básica utilizada. Estos números forman una estructura matemática definida a continuación.

Definición 4.1. *Se denomina* **semigrupo** *a la pareja* $(S, \star)$ *formada por un conjunto* S *de elementos y una operación* $\star$ *para los cuales se cumple:*

1. *El resultado de la operación* $\star$ *entre cualesquier dos elementos de* S *es también un elemento del semigrupo. Si* $a, b \in S$ *entonces* $a \star b \in S$.

2. *La operación* $\star$ *es asociativa. Si* $a, b, c \in S$ *entonces* $(a \star b) \star c = a \star (b \star c)$.

Una estructura matemática mas rica es la formada por ejemplo por los números enteros $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

Definición 4.2. *Llamamos* **grupo** *a un semigrupo* $(S, \star)$ *tal que además:*

1. *Existe un* **elemento neutro** e, *tal que para cada elemento del grupo el resultado de la operación del grupo con el elemento neutro es el mismo elemento. Tenemos pues que si* $a \in S$ *entonces* $a \star e = a$.

2. *Para cada elemento del grupo existe otro elemento del grupo, llamado su* **inverso**. *Si* $a \in S$ *entonces existe* $a^{-1} \in S$ *tal que* $a \star a^{-1} = e$.

La operación para los números enteros es nuevamente la suma, **el elemento neutro es el cero** con el cual $a + 0 = a$. El **elemento inverso** de cualquier entero a es su **negativo** $-a$ ya que $a + (-a) = 0$. Vemos que el elemento neutro es muy importante para desplazarnos libremente hacia los dos sentidos sobre la serie infinita de los números enteros.

Si queremos asociar a los años con los números enteros entonces por las razones matemáticas señaladas nos conviene mucho poder definir por ejemplo *años cero* de alguna forma. Los calendarios Juliano y de Clavius no cuentan con años cero, mientras que como podrá verse fácilmente, tanto el XIUHPOHUALLI como el TONALPOHUALLI tienen de hecho un número infinito de años cero involucrados en su estructura periódica. Es por ello que bien puede afirmarse que estos dos calendarios de ANAHUAC son superiores desde cierto punto de vista matemático tanto al calendario Juliano como al de Clavius. Estructuras periódicas bien conocidas son la hora usual, los días de la semana y los meses.

Consideremos ahora a los subconjuntos finitos de los números naturales dados por $\mathbb{N}_k = \{0, 1, 2, ..., k-1\}$, en donde k es cualquier número natural mayor que cero. $\mathbb{N}_k$ tiene entonces k elementos.

Recordemos que dado un número natural k mayor que cero, cualquier otro número natural m se puede escribir como $m = nk + r$, en donde r es un número natural mayor o igual que cero y estrictamente menor que k y n es el número natural máximo tal que $nk \leq m$ y se le llama **cociente**. Esto es $0 \leq r < k$, por lo que r puede tomar los k valores distintos $\{0, 1, 2, ..., k-1\}$. Al número r se le denomina **residuo**. Además nos percatamos que n es la **parte entera** del cociente m/k y que si n **divide** a m, lo que se escribe como $n|m$, entonces **el residuo es nulo**.

Definición 4.3. *Definamos ahora a la* **suma módulo** k *de dos números enteros* $a, b \in \mathbb{N}_k$ *misma que escribimos como* $(a+b) \bmod k$*, como el residuo que obtenemos al escribir a la suma usual de* a *con* b *en términos de un múltiplo máximo de* k*.*

La razón de introducir a las sumas módulo k es la siguiente. Si consideramos a los elementos de $\mathbb{N}_k$ y sumamos cualesquier dos de ellos como es usual obtendremos en ocasiones números que no forman parte de $\mathbb{N}_k$ lo cual no deseamos si queremos tener una estructura algebraica cerrada como la de los grupos. Sin embargo, si en lugar de usar como la operación $\star$ a la suma usual, usamos a la suma módulo k, entonces la suma módulo k de cualesquier dos elementos $a, b \in \mathbb{N}_k$ dada por $(a+b) \bmod k$ será también un elemento de $\mathbb{N}_k$. No sólo tendremos una estructura algebraica cerrada con elemento neutro, sino que para cada elemento $a \in \mathbb{N}_k$ su elemento inverso es $k-a$, dado que $((k-a)+a) \bmod k = k \bmod k = 0$, ya que $k = 1 \times k + 0$. Finalmente, el inverso del cero bajo la operación del grupo es el cero mismo. Con lo cual, todos **los conjuntos** $\mathbb{N}_k$ **forman grupos finitos Abelianos** con la operación de suma módulo k. Nuevamente vemos que el elemento neutro, el cero, es indispensable.

Y justamente son operaciones algebraicas con los elementos de grupos como $\mathbb{N}_4$, $\mathbb{N}_5$, $\mathbb{N}_{13}$, $\mathbb{N}_{18}$, $\mathbb{N}_{20}$ y $\mathbb{N}_{52}$, las que fueron evidentemente utilizadas para definir al XIUHPOHUALLI y al TONALPOHUALLI.

5. Escritura de Números

En la definición de suma módulo k de dos enteros utilizamos un resultado conocido como el **algoritmo de la división** que dice que si a y b son enteros y si $b \neq 0$, entonces existen enteros únicos q y r que satisfacen $a = qb + r$, con $0 \leq r < |b|$. Al número q se le llama el **cociente** y al número r el **residuo**. A nosotros solo nos interesa aquí el caso $b > 1$. Un resultado relacionado al algoritmo de la división que es de importancia para nosotros es la llamada **escritura de un número entero base** b, para b entero mayor que uno y que dice que para todo entero positivo no nulo a existe una y sólo una secuencia de enteros r_m, $m = 1, 2, \ldots, k$, que satisface

$$a = r_1 b^{k-1} + r_2 b^{k-2} + r_3 b^{k-3} + \ldots + r_{k-1} b^1 + r_k b^0, \qquad (1)$$

en donde $b^0 = 1$, $b^1 = b$, y $0 \leq r_m < b$ para toda $m \in \{1, 2, 3, \ldots, k\}$, con $r_1 \neq 0$.

El sistema que usamos comúnmente es el **sistema decimal** para el cual $b = 10$ y por tanto los coeficientes r_m , $m = 1, 2, \ldots, k$, son los números que cumplen $0 \leq r_m < 10$, que son los diez enteros desde el cero hasta el nueve. Sus símbolos básicos son $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, mientras que la base se define formalmente como $10 = 9 + 1$ mediante los símbolos 1 y 0 juntos. En el sistema decimal se escriben mediante yuxtaposiciones de los diez símbolos básicos o bien por medio de las potencias de 10. Así tendremos por ejemplo $2007_{10} = (2 \times 10^3 + 0 \times 10^2 + 0 \times 10^1 + 7 \times 10^0)_{10}$.

El sistema utilizado en ANAHUAC fue un **sistema vigesimal** para el cual $b = 20_{10}$. Ahora podríamos utilizar a los símbolos que se usaban en ANAHUAC, pero igualmente podemos utilizar, a los veinte símbolos alfanuméricos distintos $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, G, H, I, J\}$, y definir formalmente a la base (en decimal 20_{10}) como $10_{20} = (J + 1)_{20}$. Ahora tenemos que la expresión decimal $2007_{10} = (5 \times 20^2 + 0 \times 20^1 + 7 \times 20^0)_{10}$ está dada por la expresión vigesimal $507_{20} = (5 \times 10^2 + 0 \times 10^1 + 7 \times 10^0)_{20}$. Por simplicidad, y motivados por el uso del símbolo dado por una barra para el cinco escribiremos a los caracteres en sistemas con bases superiores a diez mediante guiones bajos, así por ejemplo en base veinte emplearemos a los símbolos siguientes

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \underline{0}, \underline{1}, \underline{2}, \underline{3}, \underline{4}, \underline{5}, \underline{6}, \underline{7}, \underline{8}, \underline{9}\}.$$

La base se encuentra ahora formalmente definida mediante $20_{10} = 10_{20} = (\underline{9} + 1)_{20}$

0 Atle, atlei[1], ahtlein[2]
1 Ce
2 Ome
3 Yei, ey(i)
4 Nahui
5 Macuilli (*de* maitl,*mano, y* cui *tomar*)
6 Chicoace, chicuace (*de* chico, *fracción, a un lado*)

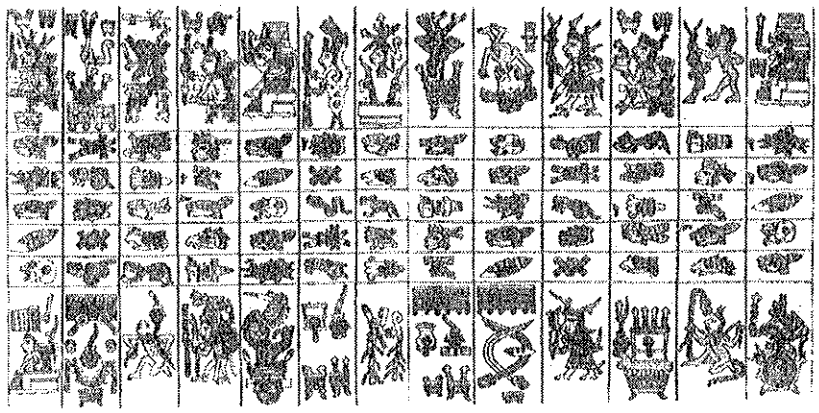
[1] *nada, o ninguna cosa*; ver [Molina]

[2] *nothing/nada, no es nada; de* ah *prefijo no*; ver [Karttunen]. Dado que lamentablemente, pese a la abundante presencia del símbolo del cero en estelas y códices, no fue de interés preservar en los diccionarios antiguos la palabra que se usó para designarlo, tan solo tenemos a la mano las palabras que designan a la nada o al conjunto vacío. No obstante, hay otras opciones para el cero citadas mas recientemente como: Xictli, según [Rodriguez]. Empero, Xictli es *ombligo, o bruxula para tirar derecho*; según [Molina]. Desde luego que el caracol o la mazorca misma pudieron ser sus designaciones, pero no hay tampoco testimonio de ello.

7 Chicome
8 Chicuey
9 Chicnahui
$10_{10} = \underline{0}_{20}$ Matlactli (*de* maitl *mano, y de* tlactli, *busto, el cuerpo de la cintura para arriba*)
$11_{10} = \underline{1}_{20}$ Matlactli ihuan ce, *o bien* matlactli once
$12_{10} = \underline{2}_{20}$ Matlactli ihuan ome, *o bien* matlactli omome
$13_{10} = \underline{3}_{20}$ Matlactli ihuan yei, *o bien* matlactli omei
$14_{10} = \underline{4}_{20}$ Matlactli ihuan nahui, *o bien* matlactli onnahui
$15_{10} = \underline{5}_{20}$ Caxtolli
$16_{10} = \underline{6}_{20}$ Caxtolli once
$17_{10} = \underline{7}_{20}$ Caxtolli omome
$18_{10} = \underline{8}_{20}$ Caxtolli omei
$19_{10} = \underline{9}_{20}$ Caxtolli onnahui
$20_{10} = 10_{20}$ Cempohualli (*del verbo* pohua, *contar*)
$21_{10} = 11_{20}$ Cempohualli once
$22_{10} = 12_{20}$ Cempohualli omome
$400_{10} = 100_{20}$ Centzontli (*de* ce,*hierba, y de* tzontli, *cabello*)
$800_{10} = 200_{20}$ Ometzontli (*dos cuatrocientos*)
$8\,000_{10} = 1\,000_{20}$ Cenxiquipilli (xiquipilli,*alforja, morral, saco, bolsa*)
$160\,000_{10} = 10\,000_{20}$ Cempohualxiquipilli (*veinte veces ocho mil*)
$3\,200\,000_{10} = 100\,000_{20}$ Centzonxiquipilli (*cuatrocientas veces ocho mil*)
$64\,000\,000_{10} = 1\,000\,000_{20}$ Cenpohualtzonxiquipilli (*veinte veces cuatrocientas veces ocho mil*)

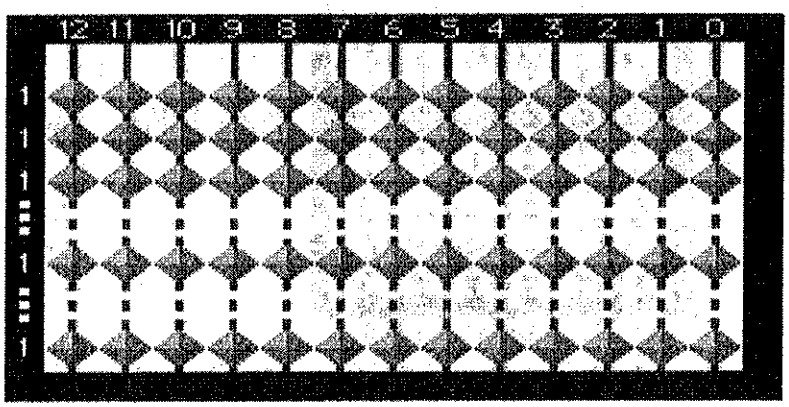
6. Instrumentos de Cálculo

Definición 6.1. *Un* **ábaco** *es un arreglo matricial de n columnas y m renglones. Sobre la columna i–ésima se encuentran f_i fichas o cuentas que pueden hallarse en g_i posiciones permitidas distintas. Aquí, $f_i < g_i \leq m$. Las fichas pueden desplazarse solamente a lo largo de las columnas siempre y cuando una posición contigua esté vacía y sea permitida. No pueden encontrarse dos o más cuentas en un mismo sitio, como tampoco cambiar su orden ni su número.*

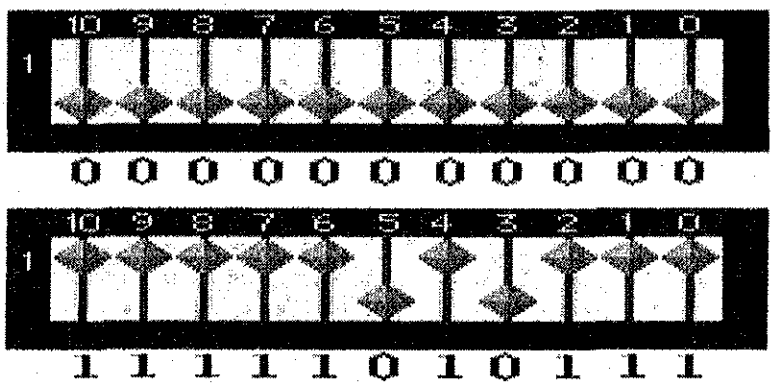


Códice Borgia. Una de las tablas o matrices del Tonalpohuali.

Aquí veremos únicamente ábacos con columnas y fichas idénticas. El ábaco mostrado en la figura siguiente tiene trece columnas iguales con b cuentas iguales cada una sobre $b+1$ posiciones permitidas, por lo que una posición estará siempre vacía.

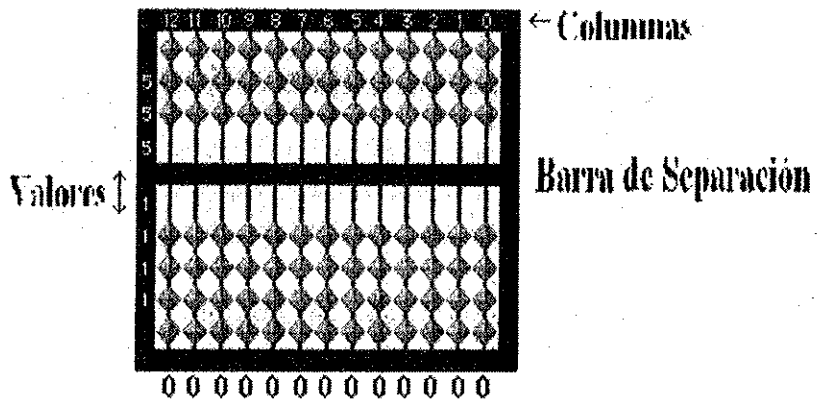


Ábaco de base fija. En este caso con trece columnas cada una con b cuentas iguales.

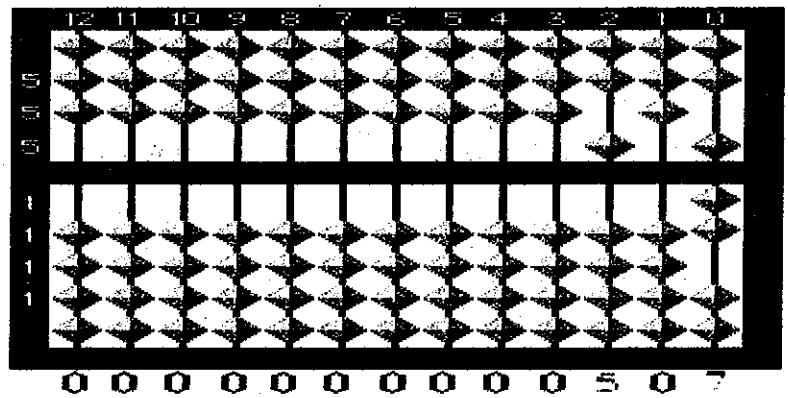


Ábaco binario o *computadora elemental.* El número cero en el de arriba y en el de abajo $(1111101011)_2 = (2007)_{10}$.

En ANAHUAC se utilizaron ábacos de base 20, nos referiremos aquí al **Nepohualtzitzin.** Se considera que surgió cerca de 900 a 1000 d.c..

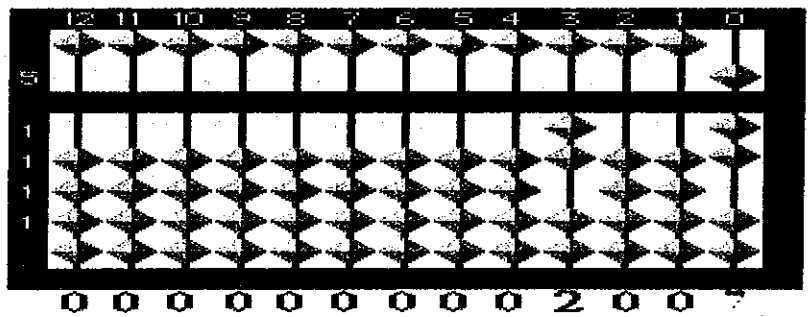


Nepohualtzitzin. Contiene en este caso trece columnas y siete renglones con valores. Aquí se encuentra representado el número cero.



Ejemplo, Nepohualtzitzin. Se representa al número $(2007)_{10}$ decimal expresado en vigesimal como $(507)_{20}$.

Dos ábacos similares, pero de base diez, son el chino *Suan pan* con cinco fichas abajo y tres arriba (con una ficha redundante arriba y abajo) y el japonés *Soroban*.



Soroban. Se representa al número 2007 decimal.

El chino se cree que se originó aproximadamente 1200 años d.c. y el japonés cerca de cuatrocientos años después via Corea.

Sistema dinámico. Tenemos un conjunto de trece casillas o celdas cada una con $b_1 + 1$ estados permitidos ϵ_i.

7. Aritmética con Ábacos.

Definición 7.1. *Un* **algoritmo** *es un conjunto finito de reglas que da una sucesión de operaciones para resolver un problema y que satisface las siguientes condiciones.*

i. Finitud*: Un algoritmo termina siempre después de un número finito de pasos.*
ii. Definitividad*: Cada paso debe estar definido precisamente, las acciones deben estar especificadas rigurosamente y sin ambigüedades.*
iii. Entrada*: Un algoritmo puede tener cero o mas* entradas*: cantidades dadas antes de que comience el algoritmo o generadas durante su desarrollo, mismas que son tomadas de conjuntos específicos de objetos.*
iv. Salida*: Un algoritmo tiene una o mas salidas, que son cantidades que tienen alguna relación con las entradas.*
v. Efectividad*: Las operaciones de un algoritmo deben ser suficientemente elementales y tales que puedan ser realizadas exactamente y en un intervalo relativamente corto de tiempo.*

El origen de la palabra algoritmo parece ser un equívoco provocado por el título de la traducción al latín de la obra *Algoritmi de numero Indorum* del matemático y astrónomo persa del siglo VIII Abdu Abdullah Muhammad ibn Musa **al-Khwarizmi**. Como ya mencionamos, no existe una definición generalmente aceptada para 'algoritmo'. No obstante, este punto es de gran interés en el estudio riguroso de las ciencias de la informática y es de gran importancia en problemas de criptología y codificación de información, por mencionar sólo dos. Ahora bien, la búsqueda de una definición de algoritmo y de la fundamentación del estudio de procesos de cálculo han pasado por muy diversas etapas, que han tenido un gran auge desde los trabajos fundamentales de Emil Post (1936) y Alan Turing (1936, 1937), sobre cuyas ideas

se basa el desarrollo actual.

Algoritmo I. Inicializar el ábaco.

I1. $j \leftarrow n$.
I2. Empujar a la ficha en la posición $(j, 1)$ hacia abajo lo más posible.
I3. Hacer $j \rightarrow j - 1$. Si $j > 0$ ir a **I1.**, en otro caso terminar. ∎

Algoritmo E. Escritura de un entero positivo.

E1. Inicializar el ábaco (escritura del cero).
E2. $j \leftarrow n$.
E3. En la columna j–ésima adicionar a_j fichas de la misma columna.
E4. Hacer $j \rightarrow j - 1$. Si $j > 0$ ir a **E3.**, en otro caso terminar. ∎

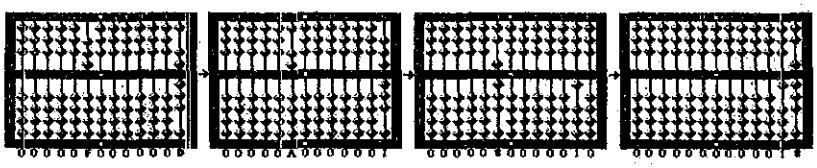
Algoritmo A. Adición de dos sumandos.

A1. Inicializar el ábaco.
A2. Escribir al primer sumando.
A3. Adicionar al segundo sumando. Esta es la operación que propiamente constituye a la acción de sumar y consta de lo siguiente.

Ai. $j \leftarrow n, k \leftarrow 0$.

Aii. En la columna j–ésima adicionar $b_j + k$ fichas libres de la misma columna. Si las fichas *si alcanzan* hacer $k = 0$. *Si faltan i fichas* regresar todas las fichas a su posición de cero, escribir $i - 1$ en la columna y hacer $k = 1$. (Esto equivale a escribir en la columna a $c_j = (a_j + b_j + k) \bmod b$, y a hacer $k = 1$ si $a_j + b_j + k \geq b$ o bien hacer $k = 0$ en otro caso.)

Aiii. Hacer $j \rightarrow j - 1$. Si $j > 0$ ir a **Aii.**, de otra forma hacer $c_0 = k$ y terminar. ∎



Suma. Nepohualtzitzin dividido en dos. En la sección derecha el primer sumando y en la izquierda el segundo.

Algoritmo R. Resta de dos enteros positivos.

R1. Inicializar el ábaco.
R2. Escribir al minuendo $(a_1 a_2 \dots a_n)_b$.
R3. Escribir al *negativo* del sustraendo de la manera siguiente.

Ri. $j \leftarrow n$, $k \leftarrow 0$.

Rii. En la columna j–ésima quitar $b_j + k$ fichas libres de la misma columna. Si las fichas *si alcanzan* hacer $k = 0$. *Si faltan i fichas*, adicionar todas las fichas de la columna a su posición con valor máximo $b - 1$, quitar $i - 1$ fchas en la columna y hacer $k = 1$. Notar que aquí $i < b$ necesariamente.

Riii. Hacer $j \rightarrow j - 1$. Si $j > 0$ ir a **Rii.**, de otra forma terminar (en este caso deberemos tener $k = 0$). ∎

8. Conclusiones

Hemos visto como el estudio de los calendarios mesoamericanos, íntimamente ligados a conocimientos astronómicos antiguos, es un tema que permite la aplicación natural de conceptos y métodos básicos de la teoría de números. Aun es menester desarrollar mas a fondo procedimientos claros que hagan posible el cálculo simple de dichos calendarios, así como mostrar explícitamente las desviaciones o errores con respecto a observaciones astronómicas sencillas. El desarrollo de algoritmos para el NEPOHUALTZITZIN es un camino viable que además permite la comprensión a fondo de un instrumento tradicional mesoamericano. Para finalizar apuntemos que problemas relevantes como lo es la computabilidad en la teoría actual de la informática, son abordados mediante el empleo de "máquinas formales", mismas que pueden ser modeladas por ábacos como los aquí tratados.

Agradecimiento Agradezco el valioso apoyo brindado por CE ACATL A.C..

Referencias

[Borgia] DÍAZ G., RODGERS A., *The Codex Borgia*, Dover Publications Inc., New York, 1993.

[Karttunen] KARTTUNEN F., *An analytical dictionary of Nahuatl*, University of Oklahoma Press, 1992.

[Knuth] KNUTH D.E., *The art of computer programming*, en dos volúmenes, Addison Wesley Publ. Co., 1981.

[Leon-Portilla] LEON PORTILLA M., *Los antiguos mexicanos*, Fondo de Cultura Económica, México, 1977.

[Meza] MEZA GUTIÉRREZ A.*El calendario de México, Cauhpohualli*, Kalpulli editorial, México, 1985.

[Meza1] MEZA GUTIÉRREZ A. *Tlapohualiztli. Principios de Matemática Ancestral*, Fundación RAC, México, sin fecha de publicación.

[Molina] MOLINA A., *Vocabulario en lengua castellana y mexicana y mexicana y catellana*, Editorial Porrúa, México, 1977.

[Morley] MORLEY S.G., *An introduction to the study of the Maya Hieroglyphs*, Dover Publications Inc., New York,1975.

[Post] Post E., contribución en *The Undecidable*, Ed. M. Davis, Raven Press, New York, 1965.

[Rodriguez] RODRIGUEZ VILLEGAS M., *Diccionario Aulex en Línea para Autodidactas. Nahuatl-Español*, 2006.

[Ruz] RUZ LLUILLIER A. *Los antiguos mayas*, Fondo de Cultura Económica, México, 2002.

[Siméon] SIMÉON R., Diccionario de la lengua nahuatl o mexicana, Siglo Veintiuno editores, México 1977.

[Smith] SMITH D.E., *History of Mathematics*, dos volúmenes, Dover Publications Inc., New York, 1958.

[Xochime] Flores Arce J.C., *Hablemos náhuatl*, Ce Ácatl A.C., México 2004.

La criptografía con clave pública, basada en gráficas

Raúl Amezcua Gómez
Universidad Autónoma Metropolitana–Azcapotzalco
Departamento de Ciencias Básicas
Av. San Pablo No. 180,
Col. Reynosa Tamaulipas
Azcapotzalco
02200 México, D.F.
rag@correo.azc.uam.mx

1. Introducción

Un sistema criptográfico es un mecanismo que permite mandar mensajes secretos. Se desarrollará en particular un sistema criptográfico de "llave pública", paradigma propuesto en la década de los 70 y que hasta la fecha es uno de los más desarrollados y aplicados hoy en día como en transferencias de dinero, control de acceso a la información archivada electrónicamente, etc.

Supongamos que la letra A significa una persona que quiere poder recibir mensajes secretos; para esto, A construye una clave pública, con la que cualquier otra persona (indicada por la letra B) puede enviarle un mensaje secreto. A puede descifrar este mensaje usando su clave secreta -la cual es diferente de su clave pública-, y que en principio solamente A conoce. La llave pública de A será conocida en particular por B, y cualquier otro que quiera enviarle mensajes secretos a A, con la cual B encriptará el mensaje que desea enviar A. Mientras tanto, podemos considerar a una persona C no autorizada o espía está tratando de descifrar el mismo mensaje encriptado sin conocer de antemano la clave secreta de A. Se han desarrollado sistemas criptográficos con llave pública basados en diferentes ideas matemáticas, aquí se presentará un ejemplo basado en conceptos de la teoría de gráficas.

2. Definiciones básicas

En este contexto, vamos a entender como *gráfica* a un conjunto de puntos o vértices y un conjunto de bordes o aristas que unen algunos de esos puntos.

Si dos vértices tienen una arista en común, decimos que son *vecinos*. La *vecindad de un vértice* consiste en el mismo vértice y todos los vértices vecinos.

Trabajaremos con gráficas que tengan la propiedad de que en ellas sea posible seleccionar un conjunto de vértices de tal modo que cualquier otro vértice sea vecino de uno y solamente de uno de los vértices seleccionados. En este caso decimos que los vértices seleccionados constituyen un *código perfecto P*. Cada vértice del código perfecto P es el centro de una *estrella*, constituida por la vecindad de un vértice de P y aristas respectivas.

Véase el ejemplo de la ilustración siguiente, en donde la gráfica de arriba tiene como vecindad del vértice 6 a los vértices 1, 2, 10, 11 y 6, y como código perfecto P a los vértices 1, 4 y 8. Observe que para construir a la gráfica con código perfecto de arriba se utilizaron las tres estrellas de abajo primero y luego se agregaron algunas aristas entre algunas puntas de estas estrellas para enmascarar a las estrellas y en última instancia los centros de las mismas (es decir, el código perfecto P).

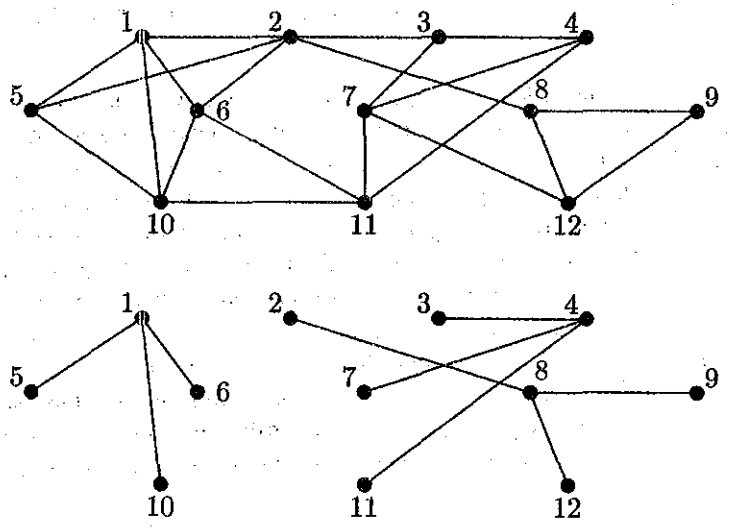


Figura 1.

El proceso de construcción de una gráfica G con un código perfecto P es unidireccional (One-way trapdoor function). Esto quiere decir que la persona que realiza la construcción de las claves G y P, clave pública y clave secreta respectivamente, va a conocer un código perfecto en la gráfica (clave secreta

P); pero una persona que tiene solamente la clave pública (G) y no ha visto el proceso de construcción de la misma (esencialmente la definición de las estrellas), tendrá mucha dificultad en general en encontrar un código perfecto en la gráfica. Una gráfica puede tener varios códigos perfectos y no todas las gráficas tienen código perfecto.

3. Criptosistema

El esquema de funcionamiento del criptosistema de clave pública desarrollado en este trabajo se describe a continuación:

1. La persona A que recibirá el mensaje secreto (la edad de B encriptada, por ejemplo) de la persona B, construye, por un lado, su llave pública que consiste en una gráfica G que contenga un código perfecto P y, por otro lado, una llave secreta que es precisamente el código perfecto P, con el cual A podrá descifrar el mensaje secreto de B cifrado por éste último por medio de la llave pública G de A.

2. La persona A puede construir su gráfica G con código perfecto P realizando los siguientes pasos.

   a) Marcar en una hoja vértices (pero no aristas), en la cual cada uno de los vértices tiene un número de identificación.

   b) Seleccionar arbitrariamente un subconjunto P de vértices. Es preferible que el subconjunto consista en aproximadamente el 20 % de los vértices. Escribir en otro papel los números de los vértices seleccionados, y guardar esta lista en secreto que será el código perfecto P de G, y en última instancia la clave secreta de A.

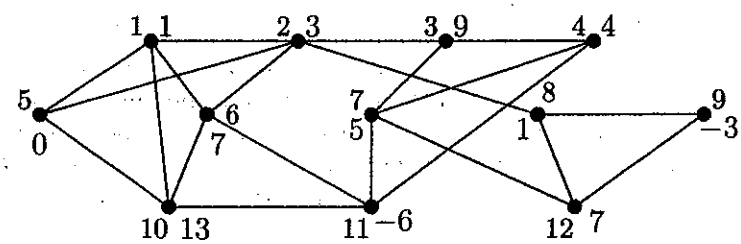
   c) Dibujar varias aristas de los vértices en P a los otros vértices, de tal modo que cada vértice esté unido únicamente a uno de los vértices del subconjunto P. En otras palabras cada vértice en P es el centro de una estrella. Los vértices que no pertenecen a P son los puntos exteriores de las estrellas.

   d) Para terminar de construir a G, dibujará aristas adicionales que unan los puntos exteriores de las estrellas unos con otros. Se puede conectar un vértice exterior de una estrella a otros vértices exteriores de la misma estrella o de otras estrellas. Pero en ningún caso construir aristas nuevas saliendo del centro de una de las estrellas. Es importante aadir un número suficiente de nuevas aristas

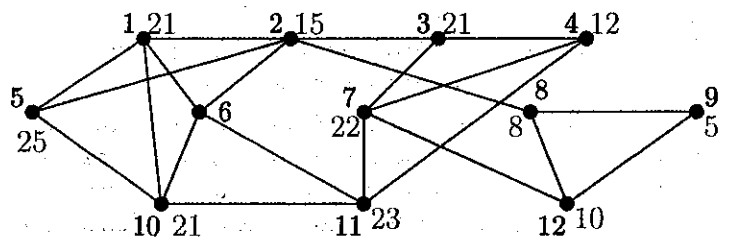
para esconder las estrellas. Es decir, al final debe ser muy difícil adivinar la ubicación de los centros de las estrellas originales.

3. Lo que B hará es asignar un número "azul" a cada vértice de la gráfica G (véase gráficas de ejemplo de la página siguiente) de tal modo que su suma sea el número N (en el ejemplo ilustrado, $41 = 1+3+9+4+0+7+5+1+(-3)+13+(-6)+7$) que quiere transmitir de manera secreta a A, luego asignará un número "verde" en cada vértice igual a la suma de todos los números azules de su vecindad y esto es lo que transmite a A. El mensaje lo descifrará A sumando sólo los números transmitidos ("verdes") por B correspondientes a los vértices del código perfecto P (del ejemplo mencionado, vértices 1, 4 y 8 -centros de las estrellas-; con números "verdes" 21, 12 y 8 asignados respectivamente, y cuya suma da 41).

4. A espera que C no logrará descifrar el mensaje encontrando la clave secreta. Esto es, A espera que el criptosistema resista el criptoanálisis de C; la dificultad de C es encontrar un código perfecto de G para determinar el número N sumando todos los números transmitidos ("verdes") que corresponden a los vértices de ese código perfecto.



Números "azules"



Números "verdes"

Figura 2.

4. Colofón

Finalmente, quiero dar crédito y aclarar que este sistema criptográfico fue mostrado por Neal Koblitz en una reunión académica en México hace ya varios años.

Criterios de Divisibilidad

Arturo Cueto Hernández
Universidad Autónoma Metropolitana–Azcapotzalco
Departamento de Ciencias Básicas
Av. San Pablo No. 180,
Col. Reynosa Tamaulipas
Azcapotzalco
02200 México, D.F.
arch@correo.azc.uam.mx

Resumen

Una de las operaciones elementales que aprendimos desde la primaria es la división, la cuál consiste en determinar el cociente y el residuo. Un primer problema que se plantea es ¿cuándo la división es exacta? es decir, ¿cuándo el residuo es cero?, esto es de interés práctico ya que en algunas situaciones basta con saber si el residuo es cero o no. Dados dos números enteros a y b, $a \neq 0$, decimos que b es divisible por a si el residuo de la división de b por a es igual a cero.

En este trabajo presentaremos algunos criterios para determinar cuando un número entero es divisible por un número primo, es decir, determinar si el residuo es cero o no sin realizar la operación de la división.

1. Introducción

Una de las operaciones elementales que aprendimos desde la primaria es la operación de dividir números enteros, la cual consiste en dados dos números enteros a y b, $a \neq 0$, hallar m y r enteros tales que

$$b = am + r$$

con $0 \leq r < |a|$.

Definición 1.1.
Sean a y b números enteros, $a \neq 0$, decimos que el número a divide a b o que b es divisible por a si existe un entero m tal que

$$b = am$$

Problema:
Dados a y b números enteros, $a \neq 0$, determinar si b es divisible por a.

Por ejemplo:

¿345 279 341 567 839 048 es divisible por 4?

¿451 987 967 978 es divisible por 4?

¿562 479 239 566 908 872 es divisible por 8?

¿371 966 587 978 es divisible por 8?

2. Congruencias

Definición 2.1.
Dos enteros a y b son congruentes respecto a un módulo m si la diferencia de ambos es divisible por m.

La definición anterior es equivalente a decir que dos enteros son congruentes módulo m si dan el mismo resto al ser divididos entre m.

Si a y b son congruentes módulo m lo denotaremos por

$$a \equiv b \pmod{m}$$

Lema 2.1.
Si a y b son congruentes módulo m entonces $b = a + km$.

Propiedades

1. Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$ entonces $a+c \equiv b+d \pmod{m}$
2. Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$ entonces $a-c \equiv b-d \pmod{m}$
3. Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$ entonces $ac \equiv bd \pmod{m}$
4. Si $a \equiv b \pmod{m}$ entonces $a^r \equiv b^r \pmod{m}$ $\forall\ r \in \mathbb{N}$

Ejemplo 2.1.
Los números 17 y 52 son congruentes módulo 7. Dado que el resto de dividir 17 y 52 por 7 en ambos casos es 3. Otra forma de ver ésto, es que su diferencia, $52 - 17 = 35$, es divisible por 7: $35 = 7 \times 5$. Así

$$17 \equiv 52 \pmod 7$$

3. Criterios para el 4 y 8

Proposición 3.1.
Un número n es divisible por 4 si y sólo si sus dos últimas cifras forman un número divisible por 4. En otras palabras, si $n = a_r a_{r-1} \ldots a_1 a_0$ y $m = a_1 a_0$

$$n \equiv 0 \pmod 4 \quad \Leftrightarrow \quad m \equiv 0 \pmod 4$$

Demostración:
Tenemos que $10 \equiv 2 \pmod 4$, luego

$$10^2 \equiv 4 \equiv 0 \pmod 4$$

Sea $b = a_r a_{r-1} \ldots a_2$, entonces

$$b \cdot 10^2 \equiv 0 \pmod 4$$

Así, si $n \equiv 0 \pmod 4$ se tiene

$$n - b \cdot 10^2 = m \equiv 0 \pmod 4$$

Ahora, si tenemos $m \equiv 0 \pmod 4$ entonces

$$m + k \cdot 10^2 \equiv 0 \pmod 4$$

Como $n = b \cdot 10^2 + m$, tenemos que

$$n \equiv 0 \pmod 4$$

□

Proposición 3.2.
Un número n es divisible por 8 si y sólo si sus tres últimas cifras forman un número divisible por 8. En otras palabras, si $n = a_r a_{r-1} \ldots a_2 a_1 a_0$ y $m = a_2 a_1 a_0$

$$n \equiv 0 \pmod 8 \quad \Leftrightarrow \quad m \equiv 0 \pmod 8$$

Demostración:
Tenemos que $10 \equiv 2 \pmod 8$, luego

$$10^3 \equiv 8 \equiv 0 \pmod 8$$

Sea $b = a_r a_{r-1} \dots a_3$, entonces

$$b \cdot 10^3 \equiv 0 \pmod 8$$

Así, si $n \equiv 0 \pmod 8$ se tiene

$$n - b \cdot 10^3 = m \equiv 0 \pmod 8$$

Ahora, si tenemos $m \equiv 0 \pmod 8$ entonces

$$m + k \cdot 10^3 \equiv 0 \pmod 8$$

Como $n = b \cdot 10^3 + m$, tenemos que

$$n \equiv 0 \pmod 8$$

□

4. Criterio para el 9

Proposición 4.1.
Un número n es divisible por 9 si y sólo si la suma de sus dígitos es divisible por 9. En otras palabras, si $n = a_r a_{r-1} \dots a_1 a_0$ y $m = \sum_{i=0}^{r} a_i$

$$n \equiv 0 \pmod 9 \quad \Leftrightarrow \quad m \equiv 0 \pmod 9$$

Demostración:
Obsérvese que $10^r \equiv 1 \pmod 9 \ \forall\ r \in \mathbb{N}$, luego

$$n = \sum_{i=0}^{r} a_i \cdot 10^i \equiv \sum_{i=0}^{r} a_i = m \pmod 9$$

Así

$$n \equiv 0 \pmod 9 \quad \Leftrightarrow \quad m \equiv 0 \pmod 9$$

□

5. Criterios para los números primos

Proposición 5.1.
Un número n es divisible por 2 si y sólo si el dígito de las unidades es 0, 2, 4, 6 u 8. En otras palabras, si $n = a_r a_{r-1} \dots a_1 a_0$ y $m = a_0$

$$n \equiv 0 \pmod 2 \quad \Leftrightarrow \quad m \equiv 0 \pmod 2$$

Proposición 5.2.
Un número n es divisible por 3 si y sólo si la suma de sus dígitos es divisible por 3. En otras palabras, si $n = a_r a_{r-1} \dots a_1 a_0$ y $m = \sum_{i=0}^{r} a_i$

$$n \equiv 0 \pmod 3 \quad \Leftrightarrow \quad m \equiv 0 \pmod 3$$

Demostración:
Obsérvese que $10^r \equiv 1 \pmod 3 \ \forall\ r \in \mathbb{N}$, luego

$$n = \sum_{i=0}^{r} a_i \cdot 10^i \equiv \sum_{i=0}^{r} a_i = m \pmod 3$$

Así

$$n \equiv 0 \pmod 3 \quad \Leftrightarrow \quad m \equiv 0 \pmod 3$$

□

Proposición 5.3.
Un número n es divisible por 5 si y sólo si el dígito de las unidades es 0 o 5.

Proposición 5.4.
Un número n es divisible por 7 cuando la diferencia entre el número sin la cifra de las unidades y el doble de la cifra de las unidades es un múltiplo de 7. En otras palabras, si $n = a_r a_{r-1} \dots a_1 a_0$ y $m = a_r a_{r-1} \dots a_1$

$$n \equiv 0 \pmod 7 \quad \Leftrightarrow \quad m - 2 \cdot a_0 \equiv 0 \pmod 7$$

Demostración:
Obsérvese que $10 \cdot m = a_r a_{r-1} \dots a_1 0$, luego

$$n - 10 \cdot m = a_0$$

Sí

$$n \equiv 0 \pmod 7 \quad \Rightarrow \quad -3 \cdot m \equiv a_0 \pmod 7$$

entonces

$$-6 \cdot m \equiv 2 \cdot a_0 \pmod 7 \quad \Rightarrow \quad m \equiv 2 \cdot a_0 \pmod 7$$

Así

$$n \equiv 0 \pmod 7 \quad \Rightarrow \quad m - 2 \cdot a_0 \equiv 0 \pmod 7$$

Supongamos ahora que

$$m - 2 \cdot a_0 = 7 \cdot k$$

entonces

$$m = 7 \cdot k + 2 \cdot a_0 \quad \Rightarrow \quad 10 \cdot m = 7 \cdot \widetilde{k} + 20 \cdot a_0$$

Como

$$n = 10 \cdot m + a_0 = 7 \cdot \widetilde{k} + 21 \cdot a_0 \equiv 0 \pmod 7$$

Así

$$m - 2 \cdot a_0 \equiv 0 \pmod 7 \quad \Rightarrow \quad n \equiv 0 \pmod 7$$

□

Proposición 5.5.
Un número n es divisible por 7 si y sólo si la suma alterna de los dígitos agrupados de tres en tres de derecha a izquierda es divisible por 7. En otras palabras, si $n = a_r a_{r-1} \ldots a_1 a_0$ y $m_j = a_{3j+2} a_{3j+1} a_{3j}$ con $j = 0, \ldots, \left[\left[\frac{r}{3}\right]\right]$

$$n \equiv 0 \pmod 7 \quad \Leftrightarrow \quad \sum_{j=0}^{\left[\frac{r}{3}\right]} (-1)^j m_j \equiv 0 \pmod 7$$

Demostración:
Obsérvese que

$$\begin{array}{lll} 10^0 \equiv 1 \pmod 7, & 10^3 \equiv 6 \equiv -1 \pmod 7, & 10^6 \equiv 1 \pmod 7, \\ 10^1 \equiv 3 \pmod 7, & 10^4 \equiv 4 \equiv -3 \pmod 7, & 10^7 \equiv 3 \pmod 7, \\ 10^2 \equiv 2 \pmod 7, & 10^5 \equiv 5 \equiv -2 \pmod 7, & 10^8 \equiv 2 \pmod 7, \end{array}$$

y así sucesivamente. Luego

$$\begin{aligned} n = \sum_{i=0}^{r} a_i \cdot 10^i \quad \equiv \quad & 2 \cdot a_2 + 3 \cdot a_1 + a_0 - 2 \cdot a_5 - 3 \cdot a_4 - a_3 \\ & +2 \cdot a_8 + 3 \cdot a_7 + a_6 - \cdots \pmod 7 \end{aligned}$$

$$n = \sum_{i=0}^{r} a_i \cdot 10^i \equiv 2 \cdot a_2 + 3 \cdot a_1 + a_0 - (2 \cdot a_5 + 3 \cdot a_4 + a_3) + 2 \cdot a_8 + 3 \cdot a_7 + a_6 - \cdots \pmod 7$$

Así tenemos

$$n \equiv a_2 a_1 a_0 - a_5 a_4 a_3 + a_8 a_7 a_6 - \cdots \pmod 7$$

es decir

$$n \equiv m_0 - m_1 + m_2 - \cdots = \sum_{j=0}^{[\frac{r}{3}]} (-1)^j m_j \pmod 7$$

Por lo tanto

$$n \equiv 0 \pmod 7 \quad \Leftrightarrow \quad \sum_{j=0}^{[\frac{r}{3}]} (-1)^j m_j \equiv 0 \pmod 7$$

□

Ejemplo 5.1.
¿6544728905663725 es divisible por 3?

Tenemos que

$$6+5+4+4+7+2+8+9+0+5+6+6+3+7+2+5 = 79$$

$$7+9 = 16 \equiv 1 \pmod 3$$

Por lo tanto, 6544728905663725 no es divisible por 3.

Ejemplo 5.2.
¿78472805420754 es divisible por 3?

Tenemos que

$$7+8+4+7+2+8+0+5+4+2+0+7+5+4 = 63$$

$$63 \equiv 0 \pmod 3$$

Por lo tanto, 78472805420754 es divisible por 3.

Ejemplo 5.3.
¿317539488 es divisible por 7?

Aplicando el primer criterio:

$$31753948 - 16 = 31753932 \rightarrow 3175393 - 4 = 3175389$$

$$\rightarrow 317538 - 18 = 317520 \rightarrow 31752 \rightarrow 3175 - 4 = 3171$$

$$\rightarrow 317 - 2 = 315 \rightarrow 31 - 10 = 21$$

$$21 \equiv 0 \pmod 7$$

Por lo tanto, 317539488 es divisible por 7.

Ejemplo 5.4.
¿39536684824 es divisible por 7?

Aplicando el segundo criterio:

$$39, 536, 684, 824$$

$$824 - 684 + 536 - 39 = 637$$

$$63 - 14 = 49$$

$$49 \equiv 0 \pmod 7$$

Por lo tanto, 39536684824 es divisible por 7.

Teorema 5.1.
Un número primo p, distinto de 2 y 5, es un divisor del número n, si éste es un divisor de la suma de sus dígitos, tomados en grupos de longitud k de derecha a izquierda, donde k es la longitud del período de la fracción $\frac{1}{p}$.

Observación: el último grupo puede tener longitud menor que k.

Demostración:
Sean k la longitud del período de la fracción $\frac{1}{p}$, t el número de grupos de longitud k, con la posibilidad de que el último tenga longitud menor, y m_0, m_1, $m_2, \ldots, m_{t-2}$, m_{t-1} los grupos de longitud k de derecha a izquierda; entonces

$$n = \sum_{j=0}^{t-1} m_j \cdot 10^{jk}$$

Dado que k es la longitud del período, tenemos que

$$10^{jk} \equiv 1 \pmod{p} \ , \ j = 0, \ldots, t-1$$

Por lo tanto

$$n \equiv \sum_{j=0}^{t-1} m_j \pmod{p}$$

Así

$$n \equiv 0 \pmod{p} \quad \Leftrightarrow \quad \sum_{j=0}^{t-1} m_j \equiv 0 \pmod{p}$$

□

Ejemplo 5.5.
¿128732472 es divisible por 37?

Tenemos que

$$\frac{1}{37} = 0.027027\cdots$$

entonces $k = 3$

$$128, 732, 472 \ \Rightarrow \ 128 + 732 + 472 = 1332$$

$$1 + 332 = 333 = 9 \cdot 37$$

Por lo tanto, 128732472 es divisible por 37.

Ejemplo 5.6.
¿7450115682700864 es divisible por 271?

Tenemos que

$$\frac{1}{271} = 0.0036900369\cdots$$

entonces $k = 5$,

$$7, 45011, 56827, 00864 \ \Rightarrow \ 7 + 45011 + 56827 + 00864 = 102709$$

$$1 + 2709 = 2710 = 10 \cdot 271$$

Por lo tanto, 7450115682700864 es divisible por 271.

6. Actividades

En las secciones anteriores hemos expuesto algunos criterios para determinar si un número es divisible por un número primo, justificando porqué éstos funcionan y dando varios ejemplos de como se emplean. Esto es tan sólo una parte del proceso "enseñanza–aprendizaje"; la parte de la exposición del tema. Otra actividad que le corresponde al docente realizar en el proceso "enseñanza–aprendizaje" es la elaboración de tareas, materiales de apoyo y cuestionarios que le permitan verificar el grado de avance del alumno.

Referente al tema tratado, criterios de divisibilidad; proponemos, a modo de ejemplo, elaborar actividades del siguiente tipo:

1. ¿Para qué valores de a es divisible el número $a234$ por 2, 3, 4, 7, 8, 9, 11?

2. ¿Para qué valores de a es divisible el número $123a$ por 2, 3, 4, 7, 8, 9; 11?

3. ¿Para qué valores de a es divisible el número $a23a$ por 2, 3, 4, 7, 8, 9, 11?

4. ¿Con qué cifra completarías para que el número sea múltiplo de a?

(a)	$12\square 2$	$a = 4$	(g)	$6\square 24$	$a = 11$
(b)	$64\square 95$	$a = 3$	(h)	$751\square$	$a = 2$
(c)	$5\square 25$	$a = 5$	(i)	$852\square$	$a = 6$
(d)	$874\square$	$a = 11$	(j)	$10\square 9$	$a = 7$
(e)	$504\square$	$a = 8$	(k)	$8\square 5$	$a = 25$
(f)	$75\square 6$	$a = 9$			

5. ¿Qué cifra hay que poner para que el número $367\square$

   a) sea múltiplo de 3 y de 5?

   b) sea múltiplo de 2 y de 5?

6. El conjunto D está formado por todos los múltiplos de dos comprendidos entre 1 y 1000; el conjunto T está formado por todos los múltiplos de tres comprendidos entre 1 y 1000. ¿Cuántos elementos tienen los conjuntos D, T y $D - T$?

7. El número N tiene este aspecto: $N = 3a42b$, con a y b dígitos. ¿De cuántas maneras puedo elegir a y b para que N sea divisible por 6?

8. ¿Cuántos números naturales de 4 cifras terminan en 36 y son múltiplos de 36?

9. Reemplazando a y b por dígitos, hallar todos los números naturales de cinco cifras $65a1b$ que son múltiplos de doce.

10. Tenemos cierta cantidad de ratones de computadora. Si los guardamos en cajas de 5, nos sobran 2; si los guardamos en cajas de 7, nos sobra 1 y si los guardamos en cajas de 3, no nos sobra ninguno. ¿Cuántos ratones tenemos?

11. Un entero a se expresa en forma decimal como $a = 3x82$ donde la cifra de las centenas x es desconocida. Calcula x para que a dé residuo 1 al dividirlo entre 9.

12. ¿Cuál es el menor múltiplo de 99, cuyos dígitos suman 99 y que empieza y termina con 97?

13. Todos los números de dos dígitos desde 19 hasta 80 se escriben en una línea sin dejar espacios. ¿Es el número así obtenido: 192021...787980 divisible entre 1980?

14. ¿Cúal es el menor número por el que debe dividirse 108675 para obtener un cuadrado perfecto?

15. Halle el número natural $A = 2^a 5^b 7^c$, sabiendo que $5A$ tiene 8 divisores más que A y que $8A$ tiene 18 divisores más que A.

16. Los libros de una biblioteca no pasan de 10000 y los podemos distribuir exactamente en lotes de 12 unidades, de 27 unidades y también de 49 unidades. ¿Cuántos libros hay exactamente en la biblioteca?

17. Al contar el número de alumnos de un colegio de 4 en 4, de 5 en 5 o de 6 en 6, resulta que siempre sobran 2. ¿Cuál es el número de alumnos, sabiendo que está comprendido entre 100 y 150?

18. Se tienen tres piezas de tela del mismo ancho, cuyas longitudes son: 180 m, 225 m y 324 m. Se desea dividir las tres piezas en lotes del mismo tamaño. ¿Cuál debe ser la longitud de estos lotes para que el número de cortes en las tres piezas sea el menor posible?

19. En cierto planeta, el nmero de días de la semana, de semanas del mes y de meses del año es el mismo. Si el año consta de 512 días, ¿cuántos días tiene una semana?

20. Sea $S = 107^{23} + 91^{46}$. ¿Cuál es el menor número primo que divide a S?

Referencias

[1] Morales Figueroa, B., Pinot Leiva, L., Suger Cofiño, E. Introducción a la Matemática Moderna. Ed Limusa. México 1981.

[2] National Council of Teachers of Mathematics. Números y sus factores. Ed. Trillas. México 1982

[3] Pérez Seguí, Ma. L. Combinatoria. Cuadernos de Olimpiadas de Matemáticas. Instituto de Matemáticas. UNAM. México 2002.

[4] Pérez Seguí, Ma. L. Teoría de Números. Cuadernos de Olimpiadas de Matemáticas. Instituto de Matemáticas. UNAM. México 2003.

[5] Rincón Mejía, H.A. Cuando Cuentes Cuántos.... Temas de Matemáticas para Bachillerato. Instituto de Matemáticas. UNAM. México 2002.

[6] Vinográdov, I. Fundamentos de la Teoría de los Números. Ed. MIR Moscú . URSS 1977.

Sucesiones, Sumas e Inducción una Invitación a la Matemática

Rogelio Herrera Aguirre
Universidad Autónoma Metropolitana–Azcapotzalco
Departamento de Ciencias Básicas
Av. San Pablo No. 180,
Col. Reynosa Tamaulipas
Azcapotzalco
02200 México, D.F.
rha@correo.azc.uam.mx

Resumen

El principio de inducción matemática, además de formar parte fundamental de la definición de los números naturales, es una herramienta de gran utilidad en el quehacer matemático, y puede ser utilizado también como una invitación, lúdica, al mundo de las matemáticas, en este trabajo, partiendo de preguntas básicas y comprensibles, se termina presentando dicho principio, buscando mostrar sus diversas facetas, y se usa, para mostrar que las matemáticas pueden ser entretenidas.

¿Qué es la vida?
Si no me lo preguntan, lo sé.
Si me lo preguntan, lo ignoro.

¿Qué es el sueño?
Si no me lo preguntan, lo sé.
Si me lo preguntan, lo ignoro.

¿Qué es la vida después del sueño?
Si no me lo preguntan, lo sé.
Si me lo preguntan, lo adivino.

Hernán Lavín Cerda

1. Introducción

Un esbozo posible, de tal acto de adivinación, dentro de las múltiples propuestas posibles, es el presente escrito, donde se plantean problemas y algunas formas de resolverlos, confiando en que se logre mostrar, que a partir de preguntas muy fáciles de enunciar y comprender, se puede llegar a problemas interesantes en matemáticas, evidenciando también, al estudiarlos, que existen diversos caminos para encontrar las respuestas buscadas.

Iniciamos en la sección 2, en particular, con un conjunto de sucesiones definidas, como se verá, mediante sumas adecuadas; en el estudio del comportamiento de estos objetos, nos percatamos de diversas formas de comprenderlos, mostrándonos a su vez la conveniencia de formalizar el concepto de Inducción Matemática, el cual se presenta en la sección 3, junto con algunos ejemplos donde se busca evidenciar, que si bien el principio mencionado es una herramienta de gran utilidad en el quehacer matemático, es de suma importancia usarlo de forma adecuada, para garantizar las conclusiones que de él obtengamos.

En la cuarta sección justificamos un par de resultados generales sobre nuestros objetos de estudio, usando para ello el Principio de Inducción, junto con algunas propiedades básicas sobre polinomios; con ayuda de estos resultados y usando nuevamente propiedades de polinomios, se justifican las expresiones para las formas de las dos últimas sucesiones, de nuestras preguntas iniciales.

Finalmente en esta sección se presenta un concepto de gran utilidad, y estrechamente relacionado con la indución, a saber el de ecuación en diferencias, junto con la conocida e importante sucesión de Fibonacci.

En la última sección se presenta un conjunto de posibles trabajos a desarrollar.

2. Sumas y sucesiones

Considere las siguientes sucesiones, de las cuales se dan los primeros diez términos, calcule el siguiente término para cada una de ellas, y una expresión general para el término n–ésimo de cada sucesión:

$1, 3, 6, 10, 15, 21, 28, 36, 45, 55,\ a_{11}, \ldots$

$2, 6, 12, 20, 30, 42, 56, 72, 90, 110,\ b_{11}, \ldots$

$1, 4, 9, 16, 25, 36, 49, 64, 81, 100,\ c_{11}, \ldots$

$1, 5, 14, 30, 55, 91, 140, 204, 285, 385,\ d_{11}, \ldots$

$1, 9, 36, 100, 225, 441, 784, 1296, 2025, 3025,\ e_{11}, \ldots$

$1, 17, 98, 354, 979, 2275, 4676, 8772, 15333, 25333,\ f_{11}, \ldots$

$1, 33, 276, 1300, 4425, 12201, 29008, 61776, 120825, 220825,\ g_{11}, \ldots$

Si nos fijamos en la primera sucesión, *ie* a_n, se puede ver que se cumple:

$$a_k - a_{k-1} = k \quad \text{para} \quad k \in \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

y como $a_1 = 1$, valor inicial, en consecuencia

$$a_{11} = 66 \quad \text{y} \quad a_n = \sum_{i=1}^{n} i$$

De manera semejante para b_n, c_n, d_n, e_n, f_n y g_n se cumplen las siguientes relaciones:

$$b_k - b_{k-1} = 2k \qquad \text{para} \quad k \in \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

$$c_k - c_{k-1} = 2k - 1 \quad \text{para} \quad k \in \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

$$d_k - d_{k-1} = k^2 \qquad \text{para} \quad k \in \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

$$e_k - e_{k-1} = k^3 \qquad \text{para} \quad k \in \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

$$f_k - f_{k-1} = k^4 \qquad \text{para} \quad k \in \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

$$g_k - g_{k-1} = k^5 \qquad \text{para} \quad k \in \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

y considerando los valores iniciales de cada caso se tiene:

$$b_{11} = 132 \quad \text{y} \quad b_n = \sum_{i=1}^{n} 2i$$

$$c_{11} = 121 \quad \text{y} \quad c_n = \sum_{i=1}^{n} (2i-1)$$

$$d_{11} = 506 \quad \text{y} \quad d_n = \sum_{i=1}^{n} i^2$$

$$e_{11} = 4356 \quad \text{y} \quad e_n = \sum_{i=1}^{n} i^3$$

$$f_{11} = 39974 \quad \text{y} \quad f_n = \sum_{i=1}^{n} i^4$$

$$g_{11} = 381876 \quad \text{y} \quad g_n = \sum_{i=1}^{n} i^5$$

De lo anterior se tiene que: a_n, b_n, c_n, d_n, e_n, f_n y g_n son respectivamente la suma de los primeros n números naturales, números pares, impares, cuadrados, cubos, potencias cuartas y potencias quintas.

En función de lo anterior usaremos en adelante las representaciones siguientes:

$$S_n \quad S_n^p \quad S_n^i \quad S_{n^2} \quad S_{n^3} \quad S_{n^4} \quad S_{n^5}$$

para cada una de las sucesiones consideradas.

A continuación se deducen expresiones que permitan calcular los valores de tales expresiones.

2.1 Para S_n se puede proceder de las siguientes formas:

a) Con el truco atribuido a Gauss (niño):

1	+	2	+	3	+	$\cdots$	+	$(n-1)$	+	n
n	+	$(n-1)$	+	$(n-2)$	+	$\cdots$	+	2	+	1
(n+1)	+	(n+1)	+	(n+1)	+	$\cdots$	+	(n+1)	+	(n+1)

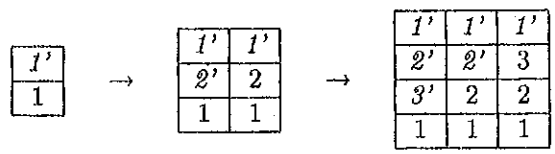
se puede observar que:

$$S_n + S_n = n(n+1)$$

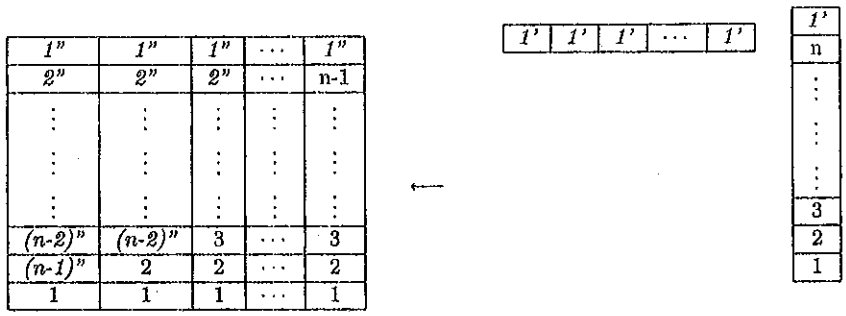
y en consecuencia:

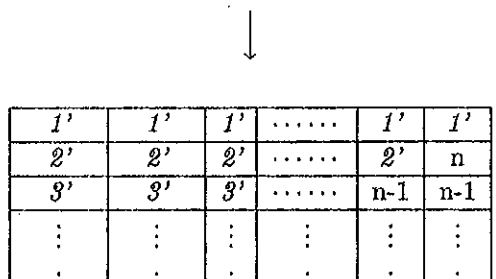
$$S_n = \frac{n(n+1)}{2} = \frac{1}{2}n^2 + \frac{1}{2}n$$

b) Otra forma de justificar el resultado es observando los siguientes tableros:



.....



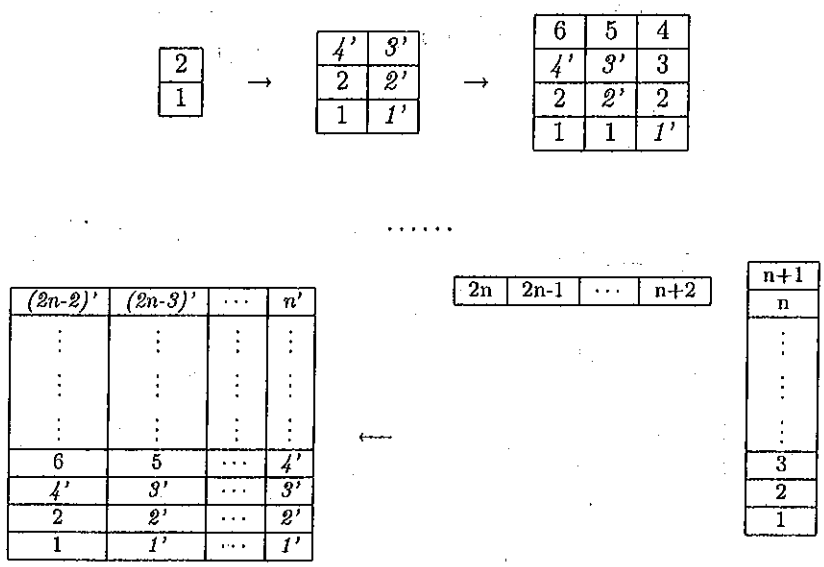


2.2 Para S_n^p se puede proceder de las siguientes formas:

a) Usando la expresión obtenida para S_n, se tienen las siguientes igualdades:

$$S_n^p = 2+4+6+\cdots+2n = 2(1+2+3+\cdots+n) = 2S_n = n(n+1)$$

b) Otra forma de justificar el resultado es observando los siguientes tableros:



2n	2n-1	2n-2	···	n+2	n+1
(2n-2)'	*(2n-3)'*	*(2n-4)'*	···	*n'*	n
⋮	⋮	⋮	⋮	⋮	⋮
6	5	4	···	*4'*	4
4'	*3'*	3	···	*3'*	3
2	*2'*	2	···	*2'*	2
1	*1'*	1	···	*1'*	1

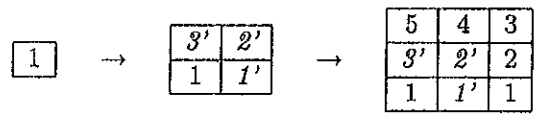
2.3 Para S_n^i puede observarse que en los diez primeros casos el valor correspondiente es el cuadrado del índice del término a calcular, luego puede conjeturarse que $S_n^i = n^2$, para justificar tal hipótesis se puede proceder de las siguientes maneras:

a) Usando las expresiones encontradas para S_n y S_n^p se tienen las siguientes igualdades:

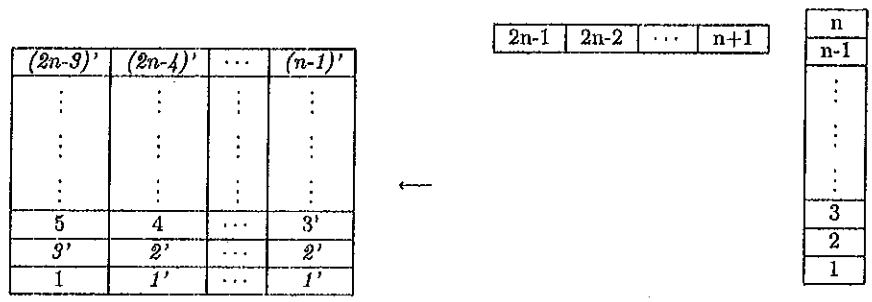
$$S_{2n-1} = S_{n-1}^p + S_n^i$$

$$S_n^i = S_{2n-1} - S_{n-1}^p = \frac{(2n-1)2n}{2} - (n-1)n = n^2$$

b) Otra forma de justificar el resultado se muestra en los siguientes tableros:



.....



2n-1	2n-2	2n-3	$\cdots$	n+1	n
(2n-3)'	*(2n-4)'*	*(2n-5)'*	$\cdots$	*(n-1)'*	n-1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
5	4	3	$\cdots$	3'	3
3'	*2'*	2	$\cdots$	*2'*	2
1	*1'*	1	$\cdots$	*1'*	1

2.4 Para S_{n^2}, se procede usando la expresión de S_n y las siguientes relaciones:

$$\begin{array}{rcccccccc}
(0+1)^3 & = & 0^3 & + & 3\cdot 0^2\cdot 1 & + & 3\cdot 0\cdot 1^2 & + & 1^3 \\
(1+1)^3 & = & 1^3 & + & 3\cdot 1^2\cdot 1 & + & 3\cdot 1\cdot 1^2 & + & 1^3 \\
(2+1)^3 & = & 2^3 & + & 3\cdot 2^2\cdot 1 & + & 3\cdot 2\cdot 1^2 & + & 1^3 \\
(3+1)^3 & = & 3^3 & + & 3\cdot 3^2\cdot 1 & + & 3\cdot 3\cdot 1^2 & + & 1^3 \\
\vdots & & & & \vdots & & \vdots & & \\
\vdots & & & & \vdots & & \vdots & & \\
(n+1)^3 & = & n^3 & + & 3\cdot n^2\cdot 1 & + & 3\cdot n\cdot 1^2 & + & 1^3 \\
\hline
S_{(n+1)^3} & = & S_{n^3} & + & 3S_{n^2} & + & 3S_n & + & (n+1)
\end{array}$$

de las identidades anteriores se sigue:

$$\begin{aligned}
(n+1)^3 &= 3S_n^2 + \tfrac{3}{2}n(n+1) + (n+1) \\
S_{n^2} &= \tfrac{1}{3}[(n+1)^3 - \tfrac{3}{2}n(n+1) - (n+1)] \\
S_{n^2} &= \tfrac{1}{6}[2(n+1)^3 - 3n(n+1) - 2(n+1)] \\
S_{n^2} &= \tfrac{1}{6}(n+1)[2(n+1)^2 - 3n - 2] \\
S_{n^2} &= \tfrac{1}{6}n(n+1)(2n+1) \\
S_{n^2} &= \tfrac{1}{3}n^3 + \tfrac{1}{2}n^2 + \tfrac{1}{6}n
\end{aligned}$$

2.5 Para S_{n^3}, se procede usando las expresiones de S_n y S_{n^2}, así como las siguientes relaciones:

$$\begin{array}{rcccccccccc}
(0+1)^4 & = & 0^4 & + & 4\cdot 0^3\cdot 1 & + & 6\cdot 0^2\cdot 1^2 & + & 4\cdot 0\cdot 1^3 & + & 1^4 \\
(1+1)^4 & = & 1^4 & + & 4\cdot 1^3\cdot 1 & + & 6\cdot 1^2\cdot 1^2 & + & 4\cdot 1\cdot 1^3 & + & 1^4 \\
(2+1)^4 & = & 2^4 & + & 4\cdot 2^3\cdot 1 & + & 6\cdot 2^2\cdot 1^2 & + & 4\cdot 2\cdot 1^3 & + & 1^4 \\
(3+1)^4 & = & 3^4 & + & 4\cdot 3^3\cdot 1 & + & 6\cdot 3^2\cdot 1^2 & + & 4\cdot 3\cdot 1^3 & + & 1^4 \\
\vdots & & & & \vdots & & \vdots & & \vdots & & \\
\vdots & & & & \vdots & & \vdots & & \vdots & & \\
(n+1)^4 & = & n^4 & + & 4\cdot n^3\cdot 1 & + & 6\cdot n^2\cdot 1^2 & + & 4\cdot n\cdot 1^3 & + & 1^4 \\
\hline
S_{(n+1)^4} & = & S_{n^4} & + & 4S_{n^3} & + & 6S_{n^2} & + & 4S_n & + & (n+1)
\end{array}$$

de las identidades anteriores se sigue:

$$\begin{aligned}
(n+1)^4 &= 4S_n^3 + n(n+1)(2n+1) + 2n(n+1) + (n+1) \\
(n+1)^4 &= 4S_n^3 + n(n+1)(2n+3) + (n+1) \\
(n+1)^4 &= 4S_n^3 + (n+1)[n(2n+3)+1] \\
&= \\
S_{n^3} &= \tfrac{1}{4}[(n+1)^4 - (n+1)(2n^2+3n+1)] \\
S_{n^3} &= \tfrac{1}{4}[(n+1)^4 - (n+1)(2n+1)(n+1)] \\
S_{n^3} &= \tfrac{1}{4}(n+1)^2[(n+1)^2 - (2n+1)] \\
S_{n^3} &= \tfrac{1}{4}[n^2(n+1)^2] \\
S_{n^3} &= (\tfrac{n(n+1)}{2})^2
\end{aligned}$$

De lo anterior observa que:

$$S_{n^3} = (S_n)^2 = \frac{1}{4}n^4 + \frac{1}{2}n^3 + \frac{1}{4}n^2$$

De manera semejante puede derivarse:

$$S_{(n+1)^5} = S_{n^5} + 5S_{n^4} + 10S_{n^3} + 10S_{n^2} + 5S_n + S_{(n+1)^0}$$

y en consecuencia:

$$S_{n^4} = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30} = \frac{1}{5}n^5 + \frac{1}{2}n^4 + \frac{1}{3}n^3 - \frac{1}{30}n$$

¿Como verificarías que esta fórmula es correcta?

Finalmente, y percatándonos de la recursividad, se tiene:

$$S_{(n+1)^{k+1}} = S_{n^{k+1}} + \binom{k+1}{1}S_{n^k} + \binom{k+1}{2}S_{n^{k-1}} + \cdots + \binom{k+1}{k}S_{n^1} + S_{(n+1)^0} \qquad (I)$$

y por lo tanto, si se han derivado:

$$S_{n^0} \qquad S_{n^1} \qquad S_{n^2} \qquad \cdots \qquad S_{n^{k-1}}$$

se puede calcular S_{n^k}.

De esta última afirmación, la cual se justificará completamente en la sección 4, se puede derivar una fórmula para S_{n^5}, pero también la derivación de esta última fórmula, como la justificación de la dada para S_{n^4}, se verán también en la sección 4.

3. Inducción

Como se anotó en la introducción, la inducción matemática es fundamentalmente una técnica que permite hacer demostraciones y definir objetos dentro de la matemática; en general existen dos métodos básicos para obtener, deducir, conocimiento; el inductivo que obtiene conocimiento "generalizando" de casos particulares, y el deductivo que deriva conocimiento "particularizando" conocimientos generales.

Si bien una primera aproximación a la adquisición de conocimiento, por parte del ser humano, es necesariamente inductiva: al observarse ciertas regularidades en un fenómeno, se aventura, mediante la formulación de una teoría, alguna predición sobre el desarrollo futuro de tal fenómeno; después de esto, necesáriamente la teoría planteada entra en un proceso de validación, que incluye, además de la comprobación de sus predicciones, construir una explicación del fenómeno a partir de la teoría, y en caso de existir teorías alternas, su confrontación con ellas; durante el proceso antes planteado, en diversos momentos, se recurre tanto a procesos inductivos como deductivos, y de esta forma el ser humano va desarrollando las teorías qué le ayudan a comprender el mundo que lo rodea.

Dentro del proceso bosquejado en el párrafo anterior, la matemática ha resultado una herramienta de gran utilidad, por no decir fundamental, y dentro de las técnicas usadas en ella una de particular importancia, es la "inducción matemática", la cual aprovecha el concepto de número natural, para formalizar, una idea primigenia del ser humano, la de regularidad, en el sentido de que si un fenómeno ha venido aconteciendo, entonces seguirá sucediendo, por ejemplo: si al final de cada día le sigue el inicio de otro, esto acontecerá "por siempre"; así debían pensar Asterix y Obelix cuando afirmaban: "lo único que debe preocuparnos, es que el cielo caiga sobre nuestras

cabezas, y esto no pasará mañana", pero si eso también "pensaron" los dinosaurios, en su momento, entonces no pudieron predecir el día que el cielo realmente cayó sobre sus cabezas.

Esta idea de regularidad en matemáticas, está representada, por ejemplo, en los puntos suspensivos, que aparecen después de los tres primeros tableros, en las justificaciones dadas para estimar: S_n, S_n^p y S_n^i, y en particular, como se anotó en el análisis realizado para S_n^i, puede observarse que los primeros diez valores para dicha sucesión son:

$$1, 4, 9, 16, 25, 36, 49, 64, 81, 100$$

de donde puede aventurarse la hipótesis de que $S_n^i = n^2$, que en este caso resulta correcta; pero en general de una afirmación hecha sobre todos los números naturales, no puede garantizarse su corrección, porqué se cumpla para algunos de ellos, considérense los siguientes ejemplos:

Ejemplo 3.1 Factoricemos, algunos de los polinomios: $x^n - 1$, en factores irreducibles dentro de $\mathbb{Z}[x]$, obteniendo:

$$\begin{aligned}
x - 1 &= x - 1 \\
x^2 - 1 &= (x-1)(x+1) \\
x^3 - 1 &= (x-1)(x^2+x+1) \\
x^4 - 1 &= (x-1)(x+1)(x^2+1) \\
x^5 - 1 &= (x-1)(x^4+x^3+x^2+x+1) \\
x^6 - 1 &= (x-1)(x+1)(x^2+x+1)(x^2-x+1)
\end{aligned}$$

de donde puede apostarse, que en tales factores de $x^n - 1$, sólo aparecen como coeficientes 1 y -1, y de hecho si seguimos calculando para los siguientes valores de n, el resultado se mantiene, pero uno de estos factores para $x^{105} - 1$, es:

$$\begin{array}{lllllllllll}
x^{48} & +x^{47} & +x^{46} & -x^{43} & -x^{42} & -2x^{41} & -x^{40} & -x^{39} & +x^{36} & +x^{35} & +x^{34} \\
 & +x^{33} & +x^{32} & +x^{31} & -x^{28} & -x^{26} & -x^{24} & -x^{22} & -x^{20} & +x^{17} & +x^{16} \\
 & +x^{15} & +x^{14} & +x^{13} & +x^{12} & -x^{9} & -x^{8} & -2x^{7} & -x^{6} & -x^{5} & +x^{2} \\
 & +x & +1 & & & & & & & &
\end{array}$$

el cual ya no cumple nuestra apuesta.

Ejemplo 3.2 Consideremos ahora el polinomio: $p(x) = x^2 + x + 41$, el cual fue analizado por L. Euler, si calculamos $p(n)$ para n entero entre cero y

nueve, obtenemos la sucesión:

$$41, 47, 53, 61, 71, 83, 97, 113, 131, 151$$

y si la revisamos, se puede observar que todos son números primos, luego puede conjeturarse que tal polinomio evaluado en enteros no negativos, dará siempre como resultado un número primo, y esto continúa así hasta $n = 39$, pero para $n = 40$ se tiene $p(40) = 41^2$, que no es primo.

Ejemplo 3.3 Los primos de Fermat, los números de la forma: $2^{2^n}+1$, fueron estudiados por P. Fermat, y se conjeturaba que para n entero no negativo siempre resultaban primos, de hecho esto es así para n entre cero y cuatro, pero para $n = 5$, se cumple:

$$2^{2^5} + 1 = 4\ 294\ 967\ 297 = (641) \cdot (6\ 700\ 417)$$

el cual por supuesto no es un número primo.

De los ejemplos presentados, debe observarse que no basta que una afirmación del tipo $\phi(n)$ con $n \in \mathbb{N}$, se cumpla en los primeros t_0 naturales, con t_0 fijo, para que valga para todo natural, si revisamos los tableros que justifican las estimaciones de: S_n, S_n^p y S_n^i, puede observarse que después de los puntos suspensivos en cada caso hay primero un arreglo en donde está representado el cálculo para $n-1$, e indicado como se va a considerar el caso n, y a continuación un tablero que muestra el caso n, esto junto con los primeros tableros completa la demostración.

Con lo anotado en el párrafo anterior, se puede introducir el siguiente resultado:

Principio de Inducción Matemática. Si se tiene una afirmación del tipo $\phi(n)$ con $n \in \mathbb{N}$, y se pueden demostrar los dos siguientes hechos:

i) $\phi(m_0)$ es verdadera para un m_0 fijo en los naturales

ii) Para cualquier $k \geq m_0$, si se cumple $\phi(k)$ entonces se cumple $\phi(k+1)$

entonces $\phi(n)$ es verdadera para todo natural mayor o igual a m_0. □

El paso i) de la definición anterior, se conoce como base de la inducción, y ii) como paso inductivo, donde suponer $\phi(k)$ verdadero, se dice que es la hipóesis inductiva.

Siguiendo esta técnica de demostración, podemos volver a justificar los resultados para S_n^i y S_{n^3}, y se podría dar una demostración de la fórmula

anotada antes para S_{n^4}, en efecto se tienen las siguientes demostraciones por inducción:

Ejemplo 3.4 Usemos inducción matemática para justificar:

$$S_n^i = \sum_{k=1}^{n}(2k-1) = n^2$$

i) $S_1^i = \sum_{k=1}^{1}(2k-1) = 1^2$.

ii) Supongamos que dado $t \in \mathbb{N}$ se cumple: $S_t^i = \sum_{k=1}^{t}(2k-1) = t^2$, entonces para $t+1$, se tiene:

$$\begin{aligned} S_{t+1}^i = \textstyle\sum_{k=1}^{t+1}(2k-1) &= \left[\textstyle\sum_{k=1}^{t}(2k-1)\right] + [2(t+1)-1] \\ &= S_t^i + 2t + 1 \\ &= t^2 + 2t + 1 \quad \text{hip. ind.} \\ &= (t+1)^2 \end{aligned}$$

□

Ejemplo 3.5 Usemos inducción matemática para justificar:

$$S_{n^3} = \sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$$

i) $S_{1^3} = \sum_{k=1}^{1} k^3 = 1^3 = \frac{1(1+1)}{2}$.

ii) Supongamos que dado $t \in \mathbb{N}$ se cumple: $S_{t^3} = \sum_{k=1}^{t} k^3 = \left(\frac{t(t+1)}{2}\right)^2$, entonces para $t+1$, se tiene:

$$\begin{aligned} S_{(t+1)^3} = \sum_{k=1}^{t+1} k^3 &= \left(\sum_{k=1}^{t} k^3\right) + (t+1)^3 \\ &= \left(\frac{t(t+1)}{2}\right)^2 + (t+1)^3 \quad \text{hip. ind.} \\ &= \tfrac{1}{4}[t^2(t+1)^2 + 4(t+1)^3] \\ &= \tfrac{1}{4}[(t+1)^2(t^2+4t+4)] \\ &= \tfrac{1}{4}(t+1)^2(t+2)^2 \\ &= \left(\frac{(t+1)[(t+1)+1]}{2}\right)^2 \end{aligned}$$

□

Ejemplo 3.6 Justificar:

$$S_{n^4} = \sum_{k=1}^{n} k^4 = \frac{1}{30} n(n+1)(2n+1)(3n^2+3n-1)$$

□

Si bien esta afirmación se puede justificar por inducción, el paso inductivo resulta demasiado engorroso, en la sección final daremos una justificación alternativa de este resultado.

El hecho de que existan demostraciones, en las que el paso inductivo sea tan complicado, que se dificulte su justificación; puede ser un indicio de que nuestro resultado no sea correcto, pero esto no siempre es verdadero, ya que existen resultados en los que el paso inductivo es aún más difícil de justificar que en el ejemplo anterior, y a pesar de esto son verdaderos, y pueden demostrarse por inducción; esto sin soslayar que existen resultados verdaderos, a los que en principio se podría aplicar el método de inducción, pero para los cuales la demostración debe usar otras técnicas.

También es importante insistir, en que el sólo paso inductivo, no puede justificar una afirmación, obsérvense al respecto, los siguientes ejemplos:

Ejemplo 3.7 Si quisiéramos, usando sólo el paso inductivo, justificar:

$$n^2 \geq 3n$$

procederíamos como sigue:

ii) Supongamos que dado $t \in \mathbb{N}$ se cumple: $t^2 \geq 3t$, entonces para $t+1$ se tiene:

$$\begin{aligned}(t+1)^2 &= t^2+2t+1 \\ &\geq 3t+2t+1 \quad \text{hip. ind.} \\ &\geq 3t+3 \\ &= 3(t+1)\end{aligned}$$

□

Ejemplo 3.8 Si quisiéramos, usando sólo el paso inductivo, justificar:

$$S_n = \frac{n^2+n+2}{2}$$

procederíamos como sigue:

ii) Supongamos que dado $t \in \mathbb{N}$ se cumple: $S_t = \frac{t^2+t+2}{2}$, entonces para $t+1$ se tiene:

$$\begin{aligned}S_{t+1} = \textstyle\sum_{k=1}^{t+1} k &= \left(\textstyle\sum_{k=1}^{t} k\right) + (t+1) \\ &= \tfrac{t^2+t+2}{2} + (t+1) \quad \text{hip. ind.} \\ &= \tfrac{t^2+3t+4}{2} \\ &= \tfrac{(t+1)^2+(t+1)+2}{2}\end{aligned}$$

□

Pero por la fórmula justificada en 2.1 sabemos que: $S_n = \frac{n(n+1)}{2}$, y claramente se tiene:

$$\frac{n(n+1)}{2} \neq \frac{n^2+n+2}{2}$$

En los dos ejemplos anteriores, al no justificarse la base de la inducción, la afirmación no se cumple para todos los naturales, pero mientras en el ejemplo 3.8 no se cumple en ningún caso, como lo justifica la última desigualdad, en el ejemplo 3.7 la afirmación: $n^2 \geq 3n$ falla para $n = 1, 2$, pero resulta verdadera a partir de $n = 3$, ya que nuestra afirmación es equivalente a:

$n(n-3) \geq 0$; y dado el paso inductivo justificado en tal ejemplo, si usamos como base $m_0 = 3$, entonces se obtiene una demostración por el método de inducción matemática, de nuestra afirmación, para todo natural mayor o igual a tres.

Es por lo anterior que en el principio de inducción matemática, la base de la inducción se da a partir de un natural m_0 fijo, el cual puede ser considerado igual a cero, o aun más se puede, saliéndose de los naturales, considerar m_0 un entero fijo, justificando entonces, si esta base se acompaña del paso inductivo, la afirmación planteada para todo entero mayor o igual a m_0.

Otro ejemplo interesante de como puede usarse la inducción, de manera incorrecta, se da a continuación:

Ejemplo 3.9 Usemos inducción matemática, para justificar la siguiente afirmación:

Los puntos de cualquier conjunto finito en el plano son colineales.

i) Si se tiene un conjunto formado por uno o dos puntos, se sigue que tales puntos son colineales.

ii) Si se supone que cada conjunto, formado por k puntos, resulta ser un conjunto de puntos colineales, entonces para todo conjunto $C_{k+1} = \{P_1, P_2, \ldots, P_k, P_{k+1}\}$, con $k+1$ puntos, se tiene que los subconjuntos: $C_k = \{P_1, P_2, \ldots, P_k\}$ y $C'_k = \{P_2, \ldots, P_k, P_{k+1}\}$, están formados sólo por k puntos, y en consecuencia, por hipótesis inductiva, existen sendas rectas l y l', que contienen a C_k y C'_k respectivamente, pero dichas rectas coinciden en los puntos P_2 y P_k, por lo tanto son la misma recta la cual contiene entonces a todo C_{k+1}, mostrando que sus puntos son colineales. □

Como se anuncio antes, en el resultado recién obtenido, se dio una aplicación incorrecta del principio de inducción, pero antes de explicar en qué consiste tal incorreción, vale la pena observar que si el resultado fuera verdadero, el plano sería en realidad una recta; basta considerar una recta l_0 contenida en el plano, y dos puntos P_1 y P_2 en dicha recta, entonces para todo punto P_0 en el plano, el conjunto de puntos $\{P_0, P_1, P_2\}$ es un conjunto finito, luego colineal y por lo tanto contenido en l_0, mostrando así que el plano se reduce a dicha recta.

En la justificación anterior de que el plano se reduce a una recta, se encuentra la clave para detectar el error cometido, en la demostración por inducción dada en 3.9, observe que lo que no es consistente con la geometría

del plano, es que dados tres puntos arbitrarios: P_0, P_1 y P_2 en el plano, estos necesariamente sean colineales, de hecho un axioma de la geometría euclidiana garantiza que en el plano existen al menos tres puntos no colineales. Si observamos ahora el paso inductivo realizado en 3.9, podemos percatarnos de que tanto C_k como C'_k, tienen cada uno al menos tres elementos, P_1, P_2 y P_k en el primer caso, y P_2, P_k y P_{k+1} en el segundo, lo cual resulta fundamental cuando aseguramos que las dos rectas encontradas, coinciden en dos puntos P_2 y P_k, que asumimos distintos para justificar que se trata de una sóla recta, así en nuestra base de la indución deberíamos justificar explícitamente que todo conjunto formado por tres puntos es un conjunto de puntos colineales, lo cual se encuentra en contradición del postulado de la geometría antes mencionado.

4. Coda

Como habíamos comentado, en esta sección damos la versión del principio de indución matemática conocido como la forma fuerte de dicho principio, en realidad ambas formas del principio son equivalentes, pero la que presentamos a continuación, facilita en algunos casos el uso del principio, para realizar demostraciones.

Principio de Inducción Matemática, forma fuerte. Si se tiene una afirmación del tipo $\phi(n)$ con $n \in \mathbb{N}$, y se pueden demostrar los dos siguientes hechos:

i) $\phi(m_0)$ es verdadera para un m_0 fijo en los naturales

ii) Para cualquier $k \geq m_0$, si se cumple $\phi(t)$ para toda $m_0 \leq t \leq k$ entonces se cumple $\phi(k+1)$

entonces $\phi(n)$ es verdadera para todo natural mayor o igual a m_0. □

Mostremos mediante algunos ejemplos la utilidad, de esta forma alternativa de nuestro principio, comenzando con la justificación de la fórmula (I), dada al final de la sección 2.

Lema 4.1 Usemos inducción matemática para justificar:

$$S_{(n+1)^{k+1}} = S_{n^{k+1}} + \binom{k+1}{1} S_{n^k} + \binom{k+1}{2} S_{n^{k-1}} + \cdots + \binom{k+1}{k} S_{n^1} + S_{(n+1)^0}$$

antes de realizar la demostración, obsérvese que la inducción se podría, en principio realizar sobre k o sobre n, nos convendrá elegir esta última opción,

así como escribir nuestra identidad como sigue:

$$S_{(n+1)^{k+1}} = \left[\sum_{j=0}^{k+1} \binom{k+1}{j} S_{n^{k+1-j}}\right] + 1$$

una vez hechas estas observaciones, procedemos a usar la técnica de inducción, como sigue:

i) Para $n = 0$, se tiene:

$$S_{1^{k+1}} = 1 = 0 + 1 = \left[\sum_{j=0}^{k+1} \binom{k+1}{j} S_{0^{k+1-j}}\right] + 1$$

ii) Si suponemos:

$$S_{(t+1)^{k+1}} = \left[\sum_{j=0}^{k+1} \binom{k+1}{j} S_{t^{k+1-j}}\right] + 1$$

entonces para $n = t + 1$, se cumple:

$$\begin{aligned}
S_{(t+2)^{k+1}} &= S_{(t+1)^{k+1}} + (t+2)^{k+1} \\
&= \left\{\left[\textstyle\sum_{j=0}^{k+1} \binom{k+1}{j} S_{t^{k+1-j}}\right] + 1\right\} + [(t+1)+1]^{k+1} \quad \text{hip. ind.} \\
&= \left[\textstyle\sum_{j=0}^{k+1} \binom{k+1}{j} S_{t^{k+1-j}}\right] + \left[\textstyle\sum_{j=0}^{k+1} \binom{k+1}{j} (t+1)^{k+1-j}\right] + 1 \\
&= \left[\textstyle\sum_{j=0}^{k+1} \binom{k+1}{j} (S_{t^{k+1-j}} + (t+1)^{k+1-j})\right] + 1 \\
&= \left[\textstyle\sum_{j=0}^{k+1} \binom{k+1}{j} S_{(t+1)^{k+1-j}}\right] + 1
\end{aligned}$$

□

Con ayuda de este resultado, podemos mostrar, usando la forma fuerte del principio de inducción, algunas propiedades básicas de S_n^k.

Lema 4.2 Para cada $k \in \mathbb{N}$, S_n^k es un polinomio, en n, de grado $k+1$, con coeficiente líder $\frac{1}{k+1}$, término constante cero, y tal que $(k+1)!S_n^k \in \mathbb{Z}[n]$,

además si $k \geq 1$ el coeficiente del término de grado k es $1/2$.

Dem. Se procede por inducción, fuerte, sobre n.

i) $S_{n^0} = n = \frac{1}{1}n$ y $1!S_{n^0} = n \in \mathbb{Z}[n]$; $S_{n^1} = \frac{1}{2}n^2 + \frac{1}{2}n$ y $2!S_{n^1} = n^2 + n \in \mathbb{Z}[n]$

ii) Supongamos que el resultado se cumple para todos los $0 \leq k < t$, entonces usando el lema 4.1, obtenemos:

$$\begin{aligned} S_{(n+1)^{t+1}} &= \left[\sum_{j=0}^{t+1} \binom{t+1}{j} S_{n^{t+1-j}}\right] + 1 \\ &= S_{n^{t+1}} + (t+1)S_{n^t} + \left[\sum_{j=2}^{t+1} \binom{t+1}{j} S_{n^{t+1-j}}\right] + 1 \end{aligned}$$

y en consecuencia, se tienen las siguientes igualdades:

$$\begin{aligned} (t+1)S_{n^t} &= (n+1)^{t+1} - \left[\sum_{j=2}^{t+1} \binom{t+1}{j} S_{n^{t+1-j}}\right] - 1 \\ S_{n^t} &= \frac{1}{t+1}(n+1)^{t+1} - \frac{1}{t+1}\left(\left[\sum_{j=2}^{t+1} \binom{t+1}{j} S_{n^{t+1-j}}\right] + 1\right) \end{aligned}$$

luego como para $0 \leq k < t$, se cumplen los resultados, entonces S_{n^t} es un polinomio de grado $t+1$, con coeficiente líder $\frac{1}{t+1}$, término constante cero, y si $t \geq 1$ el término de grado t es:

$$\frac{1}{t+1}(t+1)n^t - \frac{1}{t+1}\binom{t+1}{2}\frac{1}{t}n^t = \frac{1}{2}n^t$$

y tal que:

$$\begin{aligned} (t+1)!S_{n^t} &= (t+1)!\left\{\frac{1}{t+1}(n+1)^{t+1} - \frac{1}{t+1}\left(\left[\sum_{j=2}^{t+1} \binom{t+1}{j} S_{n^{t+1-j}}\right] + 1\right)\right\} \\ &= t!(n+1)^{t+1} - \left(\left[\sum_{j=2}^{t+1} \binom{t+1}{j} t!S_{n^{t+1-j}}\right] + t!\right) \in \mathbb{Z}[n] \end{aligned}$$

□

Con el resultado anterior, y usando el hecho de que dos polinomios de grado m, que coincidan en $m+1$ puntos, resultan ser el mismo polinomio, podemos ahora justificar la expresión para S_{n^4}, a saber:

$$S_{n^4} = \sum_{k=1}^{n} k^4 = \frac{1}{30} n(n+1)(2n+1)(3n^2+3n-1)$$

basta observar que el polinomio, anotado a la derecha coincide con los primeros seis valores de n, a partir de cero, lo cual se anota a continuación:

$$\begin{aligned}
0 &= S_{0^4} = \tfrac{1}{30}0(1)(1)(-1) \\
1 &= S_{1^4} = \tfrac{1}{30}1(2)(3)(5) \\
17 &= S_{2^4} = \tfrac{1}{30}2(3)(5)(17) \\
98 &= S_{3^4} = \tfrac{1}{30}3(4)(7)(35) \\
354 &= S_{4^4} = \tfrac{1}{30}4(5)(9)(59) \\
979 &= S_{5^4} = \tfrac{1}{30}5(6)(11)(89)
\end{aligned}$$

Para calcular ahora una expresión de S_{n^5}, podemos usar el lema 4.2, el cual nos dice que dicha expresión es un polinomio, en n, de grado seis, con término líder $1/6$, coeficiente del término de grado cinco igual a $1/2$, y término constante cero, luego tenemos la siguiente propuesta:

$$S_{n^5} = \frac{1}{6}n^6 + \frac{1}{2}n^5 + an^4 + bn^3 + cn^2 + dn$$

para determinar los valores de: a, b, c y d, se pueden usar los valores presentados al inicio del trabajo, cuando se introdujeron las sucesiones, con las que hemos venido trabajando, y obtener las igualdades siguientes:

$$\begin{aligned}
1 &= S_{1^5} = \tfrac{1}{6}\cdot 1^6 + \tfrac{1}{2}\cdot 1^5 + a\cdot 1^4 + b\cdot 1^3 + c\cdot 1^2 + d\cdot 1 \\
33 &= S_{2^5} = \tfrac{1}{6}\cdot 2^6 + \tfrac{1}{2}\cdot 2^5 + a\cdot 2^4 + b\cdot 2^3 + c\cdot 2^2 + d\cdot 2 \\
276 &= S_{3^5} = \tfrac{1}{6}\cdot 3^6 + \tfrac{1}{2}\cdot 3^5 + a\cdot 3^4 + b\cdot 3^3 + c\cdot 3^2 + d\cdot 3 \\
1300 &= S_{4^5} = \tfrac{1}{6}\cdot 4^6 + \tfrac{1}{2}\cdot 4^5 + a\cdot 4^4 + b\cdot 4^3 + c\cdot 4^2 + d\cdot 4
\end{aligned}$$

de donde obtenemos el siguiente sistema de ecuaciones:

$$\begin{aligned} a + b + c + d &= \tfrac{1}{3} \\ 16a + 8b + 4c + 2d &= \tfrac{19}{3} \\ 81a + 27b + 9c + 3d &= 33 \\ 246a + 64b + 16c + 4d &= \tfrac{316}{3} \end{aligned}$$

las soluciones de este último sistema son: $a = \frac{5}{12}$, $b = 0$, $c = -\frac{1}{12}$ y $d = 0$, y en consecuencia obtenemos la siguiente identidad:

$$S_{n^5} = \frac{1}{6}n^6 + \frac{1}{2}n^5 + \frac{5}{12}n^4 - \frac{1}{12}n^2$$

□

Terminamos este trabajo, anotando que todas las sucesiones con las que se inició el escrito cumplen con una ecuación del tipo:

$$y_{n+1} - y_n = f_n$$

donde f_n es, respectivamente: n, $2n$, $2n-1$, n^2, n^3, n^4 y n^5, dicha ecuación es un caso muy particular de ecuación en diferencias, y el conjunto de soluciones de esta ecuación, será de la forma:

$$y_n = \alpha + y_n^*$$

donde α es cualquier función constante, que a su vez de esta forma es cualquier solución de la ecuación homogénea asociada, a saber de la ecuación:

$$y_{n+1} - y_n = 0$$

y y_n^*, es una solución particular de la ecuación original, la cual en nuestro caso depende de la función f_n; la solución general de la eucación homogénea, que constituye un espacio vectorial de dimensión uno, se expresa como todos los múltiplos de: $1 = 1^t$, y esto último es debido a que 1 es solución del polinomio asociado a nuestra ecuación en diferencias, el cual es:

$$\lambda - 1 = 0$$

la expresión encontrada para cada una de nuestras sucesiones originales, corresponde a aquella solución particular que cumpla en cada caso la condición inicial, *ie* el primer valor de cada sucesión.

La teoría respecto de las ecuaciones en diferencias lineales y de coeficientes constantes, nos permite por ejemplo derivar una expresión para una

sucesión particularmente importante, la llamada sucesión de Fibonacci, la cual se define como sigue:

$$F_0 = 0,\ F_1 = 1,\ \text{y}\ F_{n+2} = F_{n+1} + F_n\ \text{ para }\ n \geq 0$$

lo primero es percatarse de que la sucesión de Fibonacci, satisface la siguiente ecuación en diferencias:

$$y_{n+2} - y_{n+1} - y_n = 0$$

la cual es homogénea, tiene dos condiciones iniciales, los primeros valores de la misma, y tiene el siguiente polinomio asociado:

$$\lambda^2 - \lambda - 1 = 0$$

luego usando la teoría correspondiente, se tiene que la solución general es:

$$y_n = \alpha\left(\frac{1+\sqrt{5}}{2}\right)^n + \beta\left(\frac{1-\sqrt{5}}{2}\right)^n$$

y que la solución que cumple nuestras condiciones iniciales es:

$$y_n^* = \left(\frac{1}{\sqrt{5}}\right)\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1}{\sqrt{5}}\right)\left(\frac{1-\sqrt{5}}{2}\right)^n$$

en la situación en que nos encontramos, en lugar de derivar este resultado, con la teoría de ecuaciones en diferencias, se puede justificar usando inducción matemática, en una variante de la forma fuerte donde necesitamos justificar nuestra base de inducción, tanto para cero como para uno, como se ve a continuación:

Lema 4.3 La forma del término general de la sucesión de Fibonacci es:

$$F_n = \left(\frac{1}{\sqrt{5}}\right)\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1}{\sqrt{5}}\right)\left(\frac{1-\sqrt{5}}{2}\right)^n$$

i)

$$0 = F_0 = \left(\tfrac{1}{\sqrt{5}}\right)\left(\tfrac{1+\sqrt{5}}{2}\right)^0 - \left(\tfrac{1}{\sqrt{5}}\right)\left(\tfrac{1-\sqrt{5}}{2}\right)^0$$

$$1 = F_1 = \left(\tfrac{1}{\sqrt{5}}\right)\left(\tfrac{1+\sqrt{5}}{2}\right)^1 - \left(\tfrac{1}{\sqrt{5}}\right)\left(\tfrac{1-\sqrt{5}}{2}\right)^1$$

ii) Supongamos que dados $t, t+1 \in \mathbb{N}$ se cumplen:

$$F_t = \left(\frac{1}{\sqrt{5}}\right)\left(\frac{1+\sqrt{5}}{2}\right)^t - \left(\frac{1}{\sqrt{5}}\right)\left(\frac{1-\sqrt{5}}{2}\right)^t$$

$$F_{t+1} = \left(\frac{1}{\sqrt{5}}\right)\left(\frac{1+\sqrt{5}}{2}\right)^{t+1} - \left(\frac{1}{\sqrt{5}}\right)\left(\frac{1-\sqrt{5}}{2}\right)^{t+1}$$

entonces para $t+2$ se tiene:

$$\begin{aligned}
F_{t+2} &= F_{t+1} + F_t \\
&= \left[\left(\tfrac{1}{\sqrt{5}}\right)\left(\tfrac{1+\sqrt{5}}{2}\right)^{t+1} - \left(\tfrac{1}{\sqrt{5}}\right)\left(\tfrac{1-\sqrt{5}}{2}\right)^{t+1}\right] \\
&\quad + \left[\left(\tfrac{1}{\sqrt{5}}\right)\left(\tfrac{1+\sqrt{5}}{2}\right)^{t} - \left(\tfrac{1}{\sqrt{5}}\right)\left(\tfrac{1-\sqrt{5}}{2}\right)^{t}\right] \\
&= \left(\tfrac{1}{\sqrt{5}}\right)\left\{\left[\left(\tfrac{1+\sqrt{5}}{2}\right)^{t+1} + \left(\tfrac{1+\sqrt{5}}{2}\right)^{t}\right] - \left[\left(\tfrac{1-\sqrt{5}}{2}\right)^{t+1} + \left(\tfrac{1-\sqrt{5}}{2}\right)^{t}\right]\right\} \\
&= \left(\tfrac{1}{\sqrt{5}}\right)\left\{\left(\tfrac{1+\sqrt{5}}{2}\right)^{t}\left[\left(\tfrac{1+\sqrt{5}}{2}\right) + 1\right] - \left(\tfrac{1-\sqrt{5}}{2}\right)^{t}\left[\left(\tfrac{1-\sqrt{5}}{2}\right) + 1\right]\right\} \\
&= \left(\tfrac{1}{\sqrt{5}}\right)\left\{\left(\tfrac{1+\sqrt{5}}{2}\right)^{t}\left(\tfrac{3+\sqrt{5}}{2}\right) - \left(\tfrac{1-\sqrt{5}}{2}\right)^{t}\left(\tfrac{3-\sqrt{5}}{2}\right)\right\} \\
&= \left(\tfrac{1}{\sqrt{5}}\right)\left\{\left(\tfrac{1+\sqrt{5}}{2}\right)^{t}\left(\tfrac{1+\sqrt{5}}{2}\right)^{2} - \left(\tfrac{1-\sqrt{5}}{2}\right)^{t}\left(\tfrac{1-\sqrt{5}}{2}\right)^{2}\right\} \\
&= \left(\tfrac{1}{\sqrt{5}}\right)\left(\tfrac{1+\sqrt{5}}{2}\right)^{t+2} - \left(\tfrac{1}{\sqrt{5}}\right)\left(\tfrac{1-\sqrt{5}}{2}\right)^{t+2}
\end{aligned}$$

□

Como puede verse en este último resultado, aun cuando el paso inductivo, puede resultar engorroso, en realidad el proponer, "adivinar", la identidad:

$$F_n = \left(\frac{1}{\sqrt{5}}\right)\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1}{\sqrt{5}}\right)\left(\frac{1-\sqrt{5}}{2}\right)^n$$

para después demostrarla por inducción, es el verdadero trabajo que requiere: imaginación, ingenio, esfuerzo; y es el que más vale la pena, por ello es importante no engañarse, y pensar que una técnica sustituye al verdadero disfrute intelectual.

5. Propuestas a desarrollar

El presente trabajo tiene como origen una plática presentada, en el Segundo Taller de Teoría de Números del Centro-Sureste, en abril de 2007, en particular dicha exposición, se dirigió a los alumnos de la Maestría en Matemáticas Educativas de la Facultad de Matemáticas de la Universidad Veracruzana, es por ello que a continuación se presentan algunas propuestas a desarrollar como posibles trabajos de tesis, que si bien están pensados para los estudiantes primero mencionados, también pueden ser desarrollados por los alumnos de la Licenciatura en Matemáticas de la misma facultad.

Propuesta 1. Realizar un estudio del papel de la Inducción Matemática en el problema de la generación de conocimiento, y en particular de su papel en la fundamentación del concepto de número natural.

Propuesta 2. Desarrollar un trabajo, sobre los polinomios que definen las sucesiones S_{n^k}, en particular sus relaciones con los números de Bernoulli, las cuales fueron estudiadas por L. Euler, buscando hacer una presentación didáctica, interesante, y que recupere el trabajo realizado por distintos matemáticos en este problema.

Propuesta 3. Desarrollar un trabajo que exponga la teoría básica de las ecuaciones en diferencias, junto con algunas de sus aplicaciones.

Propuesta 4. Realizar un estudio de la sucesión de Fibonacci, su relación con la razón dorada, y su generalización a otras, incluida la de Lucas.

Referencias

[1] Balakrishnan, V. K., Introductory Discrete Mathematics, New York: Dover Publications, inc, 1991.

[2] Bronowski, J., Los Orígenes del Conocimiento y la Imaginación, Barcelona: Gedisa, 1993.

[3] Deutsch, D., La Estructura de la Realidad, Barcelona: Anagrama, 2002.

[4] Gardner, M., Circo Matemático, Madrid: Alianza Editorial, 1985.

[5] Ribenboim, P., Clasical Theory of Algebraic Numbers, New York: Springer, 2001.

[6] Sominskii, I. S., El Metodo de la Inducción Matemática, México: Limusa, 1976.

[7] Spivak, Michael E., Calculus, Berkeley: Publish or Perish, 1980.

Memorias Segundo taller de teoría de números de centro-sureste
Se terminó de imprimir en el mes de octubre del año 2007 en los talleres de la Sección de Impresión y Reproducción de la Universidad Autónoma Metropolitana *Unidad Azcapotzalco*

La edición estuvo a cargo de la Sección de Producción y Distribución Editoriales

Se imprimieron 200 ejemplares más sobrantes para reposición.